



Sweepstakes, Lottery and Prize Scams

**A Better Business Bureau study
of how “winners” lose millions
through an evolving fraud**

BBB International Investigations Initiative

BBB Chicago bbbinfo@chicago.bbb.org

BBB Dallas info@nctx.bbb.org

BBB Omaha info@bbbinc.org

BBB San Francisco info@bbbemail.org

BBB St. Louis bbb@stlouisbbb.org

BBB International Investigations Specialist

C. Steven Baker stbaker@bbbinc.org

Issued: June 2018



Introduction

Sweepstakes, lottery and prize scams are among the most serious and pervasive frauds operating today. While the scams' roots go as far back in the culture as gambling, the fraud continues to evolve with the times. The scheme currently involves scammers telling people they have won a large amount of money in a lottery or sweepstakes, sometimes by misusing the established name of Publishers Clearing House Sweepstakes. Victims send money, purportedly for taxes or other costs that must be paid before receiving a prize. Unfortunately, the winners don't receive the promised prizes.

Nearly 500,000 people have reported this fraud to enforcement agencies in the U.S. and Canada over the last three years, and reported losses in 2017 alone totaled \$117 million. The actual number of victims and losses is likely much larger.

In 2017, 2,820 individuals reported sweepstakes and lottery scams to [Better Business Bureau \(BBB\) Scam Tracker](#), an online tool for tracking scams, with a median loss of \$500. The most frequent method of payment was wire transfer.

BBB found these frauds concentrate disproportionately on older people, who suffer the largest losses by far. A vast worldwide industry of sweepstakes mailings specifically targets older victims. Major law enforcement efforts are focused on the millions of deceptive mailings that have flooded the mailboxes of seniors across the country. In addition to money loss, victims often are emotionally devastated when they realize they have been defrauded. Some have even resorted to committing suicide.

Sweepstakes frauds involve different actors, and the methods used to contact victims have evolved from direct mail to cold calling to social media.

- BBB discovered Jamaica is a major source of "cold calls" to victims who are told they have won money. Similar calls come from Costa Rica.
- Sweepstakes/lottery fraud has become a major problem on social media. The FBI's Internet Crime Complaint Center (IC3) says about one-third of the complaints it receives about sweepstakes/

lottery fraud occur over social media. BBB receives many complaints from victims who were contacted through Facebook.

- Some fraudsters contact victims on their phones, using text messages or pop-ups on the phone browser claiming people have won large gift cards or new smartphones. The goal of this type of fraud is to gather information to sell to other scammers, and to get people enrolled in "free trial offers."
- Another major set of fraudulent actors send

mailings to victims telling them they have won a large sum of money and need to send a small amount, typically \$20, to receive their winnings.

- Mail also is used to tell people that they have won and need to call a number to learn more about their winnings. These letters also may include counterfeit checks that will supposedly cover the "fees."

Jamaica is a major player, not only for the huge numbers of U.S. and Canadian victims,

but also for the effects this is having on the people of Jamaica itself. The massive amounts of money coming into the island from lottery fraud has resulted in gang wars between rival fraud groups, who use the money to buy guns and drugs. Jamaica has about the same population as Chicago, but had more than twice the number of murders in 2017 (650 in Chicago, 1,616 in Jamaica). As a result of these problems, a State of Emergency has been declared for a large part of Jamaica, including Kingston and Montego Bay.

It's important to note sweepstakes and lotteries differ in that to enter a lottery, one must pay money to take part by buying a lottery ticket. Lotteries are illegal in the U.S. unless authorized by law. Sweepstakes, on the other hand, do not require any payment to obtain a prize. They mainly are regulated by state law. That's why most sweepstakes specifically state "no purchase required." One of the largest sweepstakes operating is Publishers Clearing House, where there is no required cost to participate. Any program that requests or receives money to award a prize, for any reason, will be considered a lottery, and therefore generally is illegal.





This study covers:

1. Introduction
2. How big is the problem?
3. Who are the victims of sweepstakes/lottery fraud?
4. Who are the primary scammers?
 - a. Calls from Jamaica
 - b. Calls from Costa Rica
 - c. Social Media from Nigeria
5. How do the scams work?
 - a. Lottery fraud online and on social media
 - b. Sweepstakes fraud via text message or mobile browser pop-up
 - c. Sweepstakes prize mailing fraud
 - d. Sweepstakes fraud by phone call
 - e. Payment
6. What's being done about it?
7. Recommendations

Readers also will learn about red flags and actions to take to prevent this type of fraud. For example, no legitimate lottery or sweepstakes will ever request money for taxes, fees or any other purpose. BBB suggests those who think they may have won a lottery or sweepstakes do a quick internet search before proceeding. Some fraud can be avoided by simply strengthening the privacy settings on social media platforms such as Facebook.

2. How big is the problem?

Complaints about sweepstakes/lottery fraud

Lottery and sweepstakes fraud is one of the most common consumer frauds operating today. Per the 2017 Federal Trade Commission's (FTC's) Consumer Sentinel Network (CSN) Data Book, sweepstakes/lottery/prize fraud was the third-most common type of fraud reported behind imposter claims (such as bogus calls from the IRS), and complaints about telephone and mobile services. For 2017, this was the third-most common complaint to the [Senate Aging Committee](#), behind IRS impersonators and robocalls. This was also number four among the top reports to BBB Scam Tracker, following phishing emails, online purchase fraud, and IRS impersonators.

Together the FTC, Internet Crime Complaint Center (IC3), and Canadian Anti-Fraud Centre (CAFC) received nearly 150,000 complaints about sweepstakes/lottery fraud in 2017, and nearly 500,000 over the last three years. Reported losses by victims totaled \$117 million in 2017 alone.

However, previous FTC studies have found less than 10 percent of fraud victims ever complain to BBB or law enforcement, meaning the actual level of fraud may be at least 10 times larger than these numbers reflect.

Many people believe this fraud is rare. But these numbers demonstrate sweepstakes/lottery fraud is incredibly common. [BBB Scam Tracker](#) allows consumers to view a heat map showing how many sweepstakes/lottery/prize fraud complaints have been made in any area in the U.S. and Canada. Consumers can see how their local areas are affected by these and other frauds.

Sweepstakes/Lottery Fraud Complaints Subset: Complaints by Complainant Age (When Reported), 2015-2017

2015 Complaints

Age	FTC		Age	IC3	
	Complaints	\$ Loss		Complaints	\$ Loss
19 & under	56	\$44,461	Under 20	5	\$2,360
20-29	558	\$135,469	20-29	48	\$87,137
30-39	821	\$186,239	30-39	51	\$152,573
40-49	1,004	\$451,362	40-49	71	\$455,888
50-59	1,857	\$1,270,668	50-59	121	\$1,011,862
60-69	2,416	\$4,179,327	Over 60	310	\$3,871,789
70+	4,408	\$19,494,932			

*IC3 discontinued complaint sharing with Consumer Sentinel in 2014

2016 Complaints

Age	FTC		Age	IC3	
	Complaints	\$ Loss		Complaints	\$ Loss
19 & under	3	\$1,365	Under 20	6	\$1,450
20-29	61	\$225,684	20-29	17	\$18,195
30-39	82	\$33,693	30-39	19	\$39,565
40-49	72	\$49,757	40-49	38	\$267,575
50-59	160	\$44,684	50-59	75	\$441,943
60-69	219	\$351,805	Over 60	244	\$4,673,020
70+	376	\$491,167			

*IC3 discontinued age reporting requirement in 2016

2017 Complaints

Age	2017 FTC		Age	2017 IC3	
	Complaints	\$ loss		Complaints	\$ loss
19 & under	8	\$1,556	Under 20	0	\$0
20-29	60	\$15,577	20-29	8	\$86,468
30-39	77	\$7,826	30-39	21	\$10,686
40-49	64	\$13,224	40-49	27	\$34,505
50-59	156	\$288,000	50-59	37	\$245,435
60-69	380	\$472,013	Over 60	189	\$1,574,134
70+	347	\$1,178,152			



Scope of Jamaican sweepstakes/lottery scams

How many of these complaints involve Jamaica? Typically, consumers may know they are dealing with schemes originating in Jamaica two ways: if they send money directly to Jamaica or if they capture a caller ID that shows the call came from area code 876. It is very difficult, however, to determine the true source. Not everyone has caller ID, and many frauds “spoof” the phone number to make it appear the call is coming from elsewhere. The Las Vegas area code 702 is a particular favorite of scammers in Jamaica.

Both Western Union and MoneyGram have made serious efforts over the last several years to combat frauds using their systems to send money directly to Jamaica.

For these reasons, there has been a recent reduction in complaints tied directly to Jamaica. Law enforcers working in this area, however, have not detected any lessening of lottery fraud activity emanating from Jamaica.

The statistics show that consumer sentinel complaints in Jamaica increased regularly for many years, declining only recently – and again, only for the reasons outlined above. More than 95 percent of reported fraud in Jamaica involves lottery or sweepstakes scams.

Reported losses to frauds in Jamaica in 2015 amounted to over \$38 million.

3. Who are the victims of sweepstakes/lottery fraud?

We know from law enforcement efforts that mass prize mailings and Jamaican lottery frauds concentrate on older people, and the available complaint data supports the thesis that this scheme disproportionately targets older populations. In addition, the FTC has found several other characteristics common to sweepstakes/lottery fraud victims.

IC3 said for those filing complaints who reported their age (they are not required to provide this information), 42

percent were over 60, but they represented 82 percent of the total losses. The CAFC in Canada also found 57 percent of complainants were over 60, representing 61 percent of total losses in 2017.

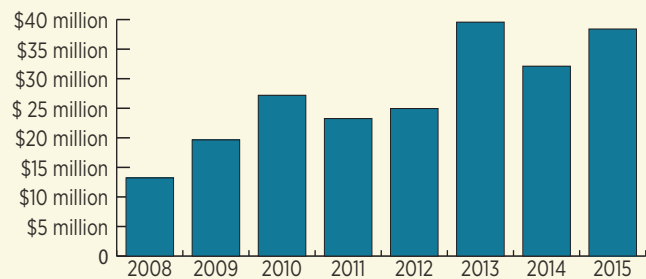
A [study released by the FTC in 2013](#) was based on a phone survey of people across the country, not just

Complaints against Jamaican Companies by Consumer Age

Age	Complaints	Amount Paid
19 and under	56	\$44,461
20-29	558	\$135,469
30-39	821	\$186,239
40-49	1,004	\$451,362
50-59	1,857	\$1,270,668
60-69	2,416	\$4,179,327
70+	4,408	\$19,494,932

From CSN 2015

CSN Complaints Against Jamaican Companies: Dollars Lost 2008 - 2015



Number of Lottery/Sweepstakes Complaints and Losses Reported to Agencies, by Year

	2015 Complaints	2015 Losses	2016 Complaints	2016 Losses	2017 Complaints	2017 Losses
FTC	151,154	\$102,946,857	159,502	\$97,361,757.00	142,870	\$95,000,000
IC3	5,324	\$19,365,223	4,321	\$21,283.77	3,011	\$16,835,001
Canada	3,723	\$6,888,364	2,157	\$3,111,867	2,026	\$2,884,332
Total	160,201	\$129,200,444	165,980	\$100,494,907.77	147,907	\$114,719,333

Total for All Years: 473,119 Complaints; \$344,414,685 Lost



complainants. It found prize promotions were the second most common type of fraud in the U.S. behind bogus weight loss products. It estimated 2.4 million adults had been victims during the previous year.

It should be noted, however, that 53% of the victims in that study had been defrauded after attending a sales presentation to get a “prize” (e.g. timeshare sales), and thus sweepstakes or lotteries were not involved. Nonetheless, FTC staff found several common factors for those who were victimized, and because the survey found similar results to those of another survey conducted several years before, the results are likely applicable today.

The survey found:

- The majority of victims were between 65-74.
- Those who had experienced a serious negative life event in the previous two years — such as divorce, death of a family member or close friend, serious family injury or illness, or loss of a job — were more than three times likely to fall victim.
- Those who had a greater willingness to take risks were more likely to be victimized.
- Those who anticipated that their income over the next three years would be the same or would decline were more likely to fall victim to a prize promotion fraud.

People may be more susceptible to sweepstakes mailings than they think. A recent [study completed at Scripps College](#) in Claremont, Calif. showed prize mailings to subjects and studied how they responded to these. Researchers found the most important factor in deciding whether to respond was the person’s assessment of the risk versus the potential reward. Almost half of their subjects indicated an interest in responding, which was more than researchers had anticipated. When the study added a requirement that people pay an activation fee of \$5 to \$100, nearly a quarter of the subjects still had an interest in responding.

Why are seniors fraud targets?

While some studies suggest older consumers are somewhat less likely to be fraud victims than the general population, perhaps because they have more life experience to guide them, there is evidence suggesting they are more likely to become victims of sweepstakes fraud. Complaint data shows more than half of victims are over 60, and those over 70 years old account for more than two thirds of the losses related to this scheme.

Why is this? It is speculated that the fraudsters hope to find victims with mild cognitive impairment, dementia or Alzheimer’s disease. These people often continue sending hundreds of thousands and even millions of dollars to fraudsters. A retired college president sent tens of thousands of dollars to scammers. [CNN](#) reported that an older man suffering from Alzheimer’s sent all of his funds to scammers and then committed suicide when the prize money never came. A [San Diego TV station](#) explains how one senior victim was defrauded.

In addition, seniors may simply have more money and

may have been at the same address, with the same phone number, for a longer time and therefore may be easier to locate.

One victim’s story: Ted

Ted was a successful businessman in St. Louis. He was originally a geological engineer, and consulted on oil drilling and made money in many other businesses. He had his own Learjet.

He never married. His mother lived with him, and he looked after her until her death. Ted is described as a “total gentleman” and was very generous with his family. He regularly taught Sunday school. He set up a fund to pay for all the college costs for his nieces and nephews.

Around 2015 Ted was in his 80s, and he was called and told he had won \$60 million. He began sending money to get his “winnings” often to Jamaica. Initially he was told that he needed to pay a transfer fee to get the money to the U.S. from Jamaica. Then Ted was told the money was in Florida, in a Brinks truck, and he needed to pay taxes on the money. After he paid, he was then told there was another tax to get the money from Florida to Georgia.

Ted continued to send money time after time. He even borrowed money from friends to pay more. Surprisingly, there were even people coming to his house to pick up money in person. Ted’s secretary changed his phone number to stop the calls and demands for money. But the fraudsters had a pizza delivered to his house. The delivery person got his new phone number, and the calls continued.

Ted’s brother moved in with him in an effort to stop the fraud from continuing. But his brother got an ulcer and had to be hospitalized, and the frauds continued to get money from Ted.

At one point, Ted asked a friend who had loaned him some money before, to loan him more because a Brink’s truck was at a local shopping mall and some funds were required to finalize the transaction. The friend offered to drive Ted to the mall, but refused to lend more money in what was clearly a fraud.

At first, Ted seemed perfectly fine, even though others realized he was a victim of a fraud.

The friend reached out to the local police, the Attorney General’s Office, and the FBI. Eventually the U.S. Postal Inspection Service got involved, and they were prepared to take action – but Ted would not press charges.

Ted didn’t really need the supposed lottery winnings. He wanted the money to donate to good causes, such as the university where he attended college.

Ted ultimately lost nearly \$8 million. At this time, he has dementia and is living in a nursing home. The advice from his friends and family? Get a conservator or guardianship and take control over the money so that the victim will still have some money to live on.



4. Who are the scammers?

Callers telling people they have won a prize

The majority of the fraudsters making this type of phone call seem to come from outside the U.S., primarily originating from Jamaica and Costa Rica. In recent years there also have been prosecutions of operations in [Canada](#) and [Israel](#). Similar operations may be located in Spain and the Philippines.

People from across the U.S. and Canada receive calls “out of the blue” informing them they’ve won a large sum of money. Scammers often ask people to confirm that they are the correct person for the award, and develop excitement by asking people what they will do with their winnings. Often scammers ask if it is okay to have a photographer or TV crew present when they deliver the check. They instruct victims to keep this secret “to prevent fraud.”

After several minutes of conversation, and after people get committed to the idea something important is going to change in their lives, scammers spring the trap: taxes must be paid and received before the check can be delivered. Victims are urged to move quickly and send money, often through Western Union or MoneyGram. Although the amounts requested vary a great deal, they will be at least several hundred dollars.

These callers often pretend to be from Publishers Clearing House, which does have a sweepstakes, but reports that they never call winners in advance and never requires that winners pay any money to receive the money. Other callers may claim to be with Mega Millions, which is a joint effort of many state lotteries. Since that is a lottery, no one can win unless they have bought a lottery ticket.

Those who pay once are then usually asked for more money for some supposed error or problem. Some of these include claims they were driving to the victim’s house but got stopped by the police or tax authorities, or that victims must pay for security guards to accompany the money.

In these scams, no one ever wins and the requests for money can continue for a very long time.

A. Jamaica

There are a few hallmarks of callers from Jamaica. They often impersonate the Publishers Clearing House Sweepstakes, calling people to tell them they have won a large prize. Another giveaway of fraud originating in Jamaica is the phone number used in fraudulent calls. Jamaica’s area code is 876. Jamaican frauds also often claim that a new Mercedes Benz will be delivered to the victim later in the day. It may be that this creates an additional sense of urgency to get the victim to send money right away. Here is the [FTC warning about lottery fraud from Jamaica](#). CNBC’s [American Greed](#) aired a story on this problem.

Why Jamaica?

Jamaica is an English-speaking country and has been used by U.S. companies in the past to outsource customer service phone operations. This seems to have provided telemarketing training to some residents. The focus of this fraud in Jamaica has been St. James Parish, but it has been expanding into other areas.

When frauds are successful, they tend to grow quickly as more people learn how to operate them. Telemarketers break off and form their own operations, hiring additional people and increasing the amount of fraud. Scammers tend to operate in places where they believe there is little risk of criminal prosecution. In addition, the money provided by any fraud can at times be used to corrupt public officials or to support other types of crime.

Sanjay Williams

The case of Sanjay Williams provides a good illustration of how a Jamaican sweepstakes/lottery fraud works. Williams, a Jamaican, seems to have begun his career making telephone calls to older people in the United States. Federal authorities allege that he had over 80 victims, with total victim losses of more than \$5.5 million. Williams told his prospective senior victims that to get their prize winning, they needed to pay fees for taxes, insurance, or other reasons. At least one victim lost \$850,000. Williams also used threats of violence against victims and their families to extort more money. He told one victim he would kill their sons and rape their daughters. Another of Williams’ victims committed suicide.

Williams then decided to get into the lead list business, selling contact information of potential victims to other fraudsters. He apparently sought leads with information on people who had responded to mailings promising that they had won a large sum of money and simply needed to send back \$20 or so in order to obtain their winnings. Williams was buying these leads in the U.S. for as much as \$5.50 per name and sold them to his co-conspirators and some 400 other fraudsters in Jamaica.

He was arrested when he visited the U.S. to obtain leads, and was prosecuted by the U.S. Attorney’s office in the District of North Dakota,

which has concentrated on Jamaican fraud. The FBI and Postal Inspection Service are credited with doing the supporting investigation. A representative of Jamaica’s Major Organised Crime and Anti-Corruption Agency (MOCA), Lottery Scam Task Force testified at the trial as an expert witness. An official from MOCA in Jamaica emphasized the willingness of Jamaican law enforcement





officials to continue to work in partnership with their United States counterparts to fight the ongoing scourge of lottery fraud, and to assist in the efforts to bring the remaining indicted Jamaican defendants to trial in North Dakota.

Williams was **convicted by a jury**. On Nov. 24, 2015, he was **sentenced** to 20 years in federal prison and ordered to pay \$5.6 million in restitution to victims.

The impact of Jamaican fraud on the country

The fraud originating from Jamaica is especially troubling, not only for the sheer number of victims in the U.S. and Canada but also because it has led to a major upsurge in violence rocking Jamaica.

The massive amounts of money coming into the island from lottery fraud has resulted in gang wars between rival fraud groups, who are also using the money to buy guns and drugs. Jamaica had more than twice the number of murders in 2017 as Chicago, and more than five times as many murders as New York. **One California woman died in Jamaica in 2017, seemingly as a result of a lottery scam.**

A recent **State Department report** states, “There are dozens of violent Jamaican gangs on the Island. Jamaica continues to experience a large number of financial crimes related to cybercrimes and advance fee fraud (lottery scams), which primarily target U.S. citizens.”

The sweepstakes/lottery problem may have contributed to the state of emergency for much of the island. In January 2018, the State Department issued a travel warning for St. James Parish (which includes Montego Bay) and Kingston, the two biggest cities in Jamaica. This has since been extended to other parts of Jamaica.

As the State Department puts it: “The State of Emergency, declared under the 1966 Emergency Powers Act, allows Jamaican security forces within the borders of St. James Parish to arbitrarily detain and deport suspicious persons, enter premises, and seize property without warrant. Expect to encounter increased police and military presence, checkpoints, and searches of persons and vehicles within the borders of St. James Parish.”

Other States of Emergency have since been declared in other Jamaican parishes and will remain active through the summer. These steps seem to have broad public support in Jamaica.

Working with a limited budget, Jamaican law enforcement officials have executed search warrants and arrested hundreds of those involved in lottery fraud in Jamaica. Law enforcement officials are working hard on this problem, trying to educate the Jamaican public about these issues and attempting to warn younger people there about the pitfalls of lottery scamming. Jamaican police have **produced a video** urging Jamaicans to help stop lottery fraud.

Luis Moreno, the U.S. Ambassador to Jamaica, has made **attacking lottery fraud** one of his priorities. “If we do not do more, the cultural and economic distortion that this dirty money brings could destroy a whole generation,” says Moreno.

B. Costa Rica

A sizable lottery fraud industry with dozens of call centers has been operating from Costa Rica for some years. It is home to many people originally from the U.S., some avoiding arrests for other crimes. Native English speakers may make these calls more effective. Costa Rican citizens cannot be extradited, and it is possible to get Costa Rican citizenship in two years if someone is married to a Costa Rican citizen.

Hallmarks of Costa Rica lottery fraud

Costa Ricans tend to use internet phones, known as Voice Over Internet Protocol (VOIP), and typically use technology to “spoof” the caller ID and make the calls look like they are coming from within the U.S. Many of these display area code 202, which covers the Washington, DC area.

These callers often claim to be calling from U.S. law enforcement, often using the names of real people from the FBI, Homeland Security, the FTC and the Consumer Financial Protection Bureau. Costa Rican fraudsters falsely tell victims there is so much fraud with lotteries and sweepstakes that law enforcement agencies have taken over notifying winners so that people can be assured it is legitimate.

5. How do the scams work?

Many people believe lottery or sweepstakes frauds could never happen to them. Most fraud victims are regular people whose tools for detecting deception simply didn't work well against the frauds. Why is that?

The crooks are professionals. Every detail of the fraud is carefully created by full-time professional fraudsters. They have scripted answers for any question posed to them. They tell people they must take action immediately or the award will be given to someone else. Many find it difficult to detect deceit by talking to the crooks over the telephone. Consumers may be able to detect small inconsistencies, but the idea that the entire transaction is a total fraud, the “Big Lie” propaganda technique, is more than many people can grasp.

They tell people something they want to believe. Millions of people buy lottery tickets and enter sweepstakes. People like to believe it is their turn to win. Interviews with victims show they are not overcome with greed. Rather, scammers encourage them to think about the nice things they can do for their families or communities with the money. Perhaps they want to help out a relative in financial distress, or have a grandchild who wants to go to college. For many seniors, it may be a way to increase their importance in the lives of their families.

Victims are told to keep this secret. Crooks caution victims they must not tell anyone about the award before they receive their winnings. This makes it less likely the victim will consult with someone before sending money.

Some victims keep sending money. The complaints show most victims lose money once and then move on. Some chronic victims, called “whales” by scammers,



just keep sending money. These victims are told to pay various fees for taxes, insurance, courier fees, airport taxes, document fees or other reasons, usually over several weeks, months or even years. Some consumers have lost hundreds of thousands of dollars, even millions in some cases, in a vain attempt to collect their “winnings.”

The skilled fraudsters learn all they can about an elderly victims’ assets and ability to borrow cash, take advances on credit cards, obtain loans on their homes or cars or even cash out stocks or other retirement savings. The scammer may even pretend to put in their own money as an advance to help pay those taxes. Scammers have sent flowers and birthday cards, often calling daily, which may be more contact than the victims has with real family or friends. These chronic victims believe the scammer is a true friend, and the relationship they have with them is real.

Threats. Jamaican lottery fraudsters sometimes threaten physical violence against those who refuse to send more money. These threats often are effective. Scammers may use Google Earth to look at an actual picture of the victim’s house. They can then call the victim and describe the house in detail, such as, “You live in the green house on the corner with white shutters.” They may claim to be nearby, perhaps directly across the street. They sometimes threaten the victims or their families with physical violence if they do not send more money.

Sunk costs. When people send money, they become invested in the transaction and often believe sending just a little more will produce the money they are promised. This may be true especially when family members, their bank, and local authorities have warned the victim that it is a scam. Scammers encourage victims to trust them instead and send more money, reassuring victims they are smarter than those attempting to warn them, which will be proven when the funds arrive. Thus the loss numbers can increase dramatically over time.

One victim’s story: Shirley

Shirley is retired from the Social Security Administration. She is 84 and lives in a senior center in a small town near Rockford, Ill. She does not normally get involved with matters like this. She does not even buy lottery tickets.

In May 2016 she got a phone call from James Millions, who said he was with a company called International Gaming Board and Luxury Co. Millions told her she had

won a \$2.5 million sweepstakes. He also said she had won a new Mercedes. He made the whole thing sound very exciting. But he told her she had to send money for the taxes owed on this money. She sent \$400 through Western Union from a local pharmacy.

Shirley thought the money would be useful. She thought the winnings would help her son and daughter. She also hoped to donate money to a charity for disabled children.

The next day she received another call from Millions. He said he was driving to her home from Chicago and had been stopped by the police. So he said he needed her to send some money so he could deliver the check. She complied.

Over the next several weeks Shirley received more calls asking for money so her winnings could be delivered. She ultimately sent about \$4,000. Sometimes she was told to put cash in packages and mail them. She sent express mail with money in it to Jamaica, Cincinnati, and Gainesville, Fla. In addition, she made a number of long-distance calls to the sweepstakes company in Jamaica, and ran up an \$800 phone bill. Every time it seemed like there was just one more simple step to actually receiving the winnings, and the callers convinced Shirley that the money was real and she was going to receive it.

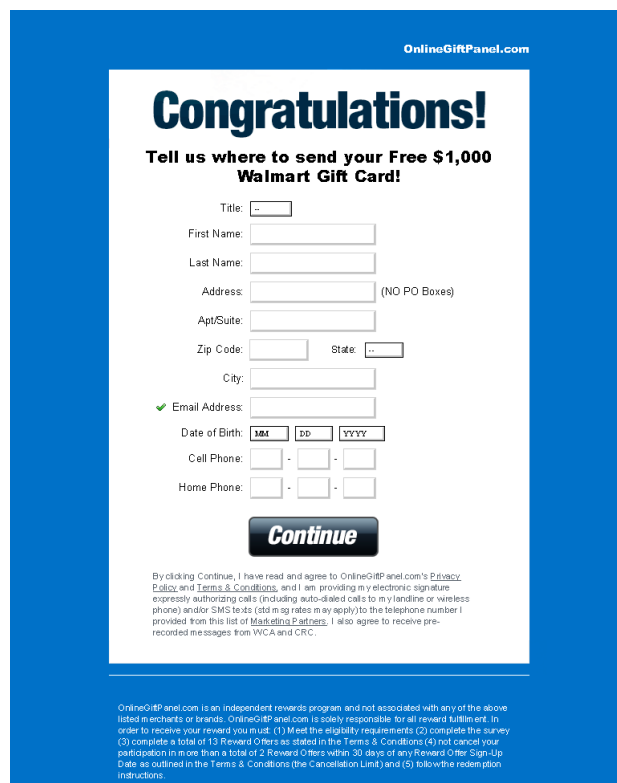
She was worried this might be a fraud and called BBB. She was informed that it was a fraud. She stopped sending money, and the calls to her stopped.

Her advice? “If you have to pay money to get a prize, it’s fraud.”

A. Lottery fraud online and on social media

Criminals also are actively using social media to find victims. IC3 says a third of the sweepstakes fraud complaints they receive involve social media. IC3 also found that of social media sweepstakes fraud victims who provided their age, 60 percent were 60 years old or older. Reports to BBB’s Scam Tracker of lottery scams over social media most frequently cite Facebook as the social media network involved. Social media companies generally do not themselves operate a lottery or sweepstakes, and any message saying they do is almost certainly a fraud.

When users fail to set secure privacy settings, scammers can find victims through social media platforms like Facebook. Facebook’s private messaging app, Messenger, is used extensively in social media sweepstakes scams. Messenger can be used with or without a Facebook profile and can be used to contact users who are not Facebook



OnlineGiftPanel.com

Congratulations!

Tell us where to send your Free \$1,000 Walmart Gift Card!

Title:

First Name:

Last Name:

Address: (NO PO Boxes)

Apt/Suite:

Zip Code: State:

City:

✓ Email Address:

Date of Birth:

Cell Phone: - -

Home Phone: - -

Continue

By clicking Continue, I have read and agree to OnlineGiftPanel.com's Privacy Policy and Terms & Conditions, and I am providing my electronic signature expressly authorizing calls (including auto-dialed calls to my landline or wireless phone) and/or SMS texts (SMS msg rates may apply) to the telephone number I provided from this list of Marketing Partners. I also agree to receive pre-recorded messages from WCA and CRC.

OnlineGiftPanel.com is an independent rewards program and not associated with any of the above listed merchants or brands. OnlineGiftPanel.com is solely responsible for all reward fulfillment. In order to receive your reward you must: (1) Meet the eligibility requirements (2) complete the survey (3) complete a total of 10 Reward Offers as stated in the Terms & Conditions (4) not cancel your participation in more than a total of 2 Reward Offers within 30 days of your Reward Offer Sign-Up Date as outlined in the Terms & Conditions (the Cancellation Limit) and (5) follow the redemption instructions.



friends. Users who are not aware of how data is stored in Facebook and Messenger may be particularly vulnerable to being targeted in lottery scams through social media.

Social media lottery fraud

There are two main variations of lottery fraud operating on Facebook, through other apps by Facebook and other social media.

Facebook Messenger lottery fraud

In the first variation, users may be contacted through Facebook Messenger by a fraudster who claims to be a prize company, a Facebook employee or Facebook founder Mark Zuckerberg. Other scammers may even impersonate people who really did win major state lotteries, claiming they want to give away some of their money to deserving individuals. The target is told they've won a "Facebook lottery," and is instructed to send money or a gift card to claim their prize. Even if the users send the money, there is no award.

There is no Facebook lottery, and neither Zuckerberg nor other lottery winners are giving money away to random people. **Facebook has a warning about such frauds.** Some victims continue to believe they are dealing with Facebook even after they have lost their money, believing it was Facebook, rather than the scammer, that failed to deliver the winnings. The **New York Times** recently looked at sweepstakes frauds operating on Facebook and found 208 fake profiles on Facebook and Instagram impersonating Zuckerberg or COO Sheryl Sandberg. At least 51 of these were being used for lottery scams. Facebook took them down the next day after being notified.

"These scams violate our policies and have no place on Facebook," Pete Voss, Facebook spokesperson, said. "We have a dedicated team and automated systems to help detect and block these kinds of scams. If you see a post or message that tries to trick you into sharing personal information or sending money, please report it using the tools we provide at facebook.com/report."

Winners list lottery fraud

A second tactic, frequently reported to BBB's Scam Tracker, is for someone to be told by a scammer who is impersonating a friend that the "friend" won a lottery, and saw the target's name was on the list of winners as well. The fraudster tells their target to send a message to a "Facebook employee" to obtain the money. When the victim reaches out, they're asked to pay a fee to obtain their prize.

When the fraudster contacts the original users' friends to tell them about their own supposed lottery winning, it goes a long way in enhancing the credibility of the claim.

How do they make it appear that this message is coming from a real friend?

- The fraudsters can copy the profile of a Facebook user, including the profile picture, and set up a cloned profile that appears to be the user's. They may reach out to the user's friends with the cloned

profile, asking to be added as a Facebook friend. It is easy to make an excuse for why they need to be friended again, such as a computer glitch. It is common for people to quickly accept the request because they believe it is someone they know already. If the target accepts the cloned profile friend request, the owner of the cloned profile can view and contact all of the target's other friends.

- Fraudsters can simply take over a user's Facebook profile. The login credentials of many Facebook users **can be purchased for as little as \$5.20** on the dark web.

Why do these tactics work? Many people have heard of businesses giving awards to customers, such as the millionth visitor at a store, for example. Most people would not abandon a chance to win \$500,000 when all they have to do is contact someone to check it out. Most believe that with just a little caution, they would be able to quickly spot a scam.

Those who do respond quickly run into a very organized and seemingly legitimate fraud, often using official-looking language and even fake websites that look real. Some believe that sending a couple of hundred dollars is worth the potential reward, even if it does turn out to be fraudulent. Moreover, this fraud is done on such a wide scale that if even a small percentage of people respond and send money, the scheme is still profitable.

There are **reports** that Facebook is taking efforts to remove fake profiles from its platform, and that it had

John, you're almost done! Your Progress:

LAST STEPS

Congratulations! To qualify for your Free \$1,000 Walmart Gift Card start by fully completing any 2 reward offers below!

Once you fully complete the offer eligibility requirements as outlined in the terms and conditions, an email message will be sent to your registered email address to confirm shipping details.

Reserved for:

Complete Any 2 Offers Below to Claim Your Gift

<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p style="text-align: center; font-size: small;">CreditReport.com</p> <div style="text-align: center; background-color: #007bff; color: white; padding: 5px; margin-bottom: 10px;"> Get your FREE Credit Score </div> <p style="text-align: center; font-size: x-small;">CreditReport.com</p> <p style="font-size: x-small;">Get your FREE Credit Score with enrollment in CreditReport.com. It's easy to read and you can view it online in seconds. Stay protected with the state-of-the-art credit monitoring tools!</p> <p style="text-align: center; background-color: #dc3545; color: white; padding: 5px; border-radius: 5px;">Get Your Credit Now</p> </div>	<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p style="text-align: center; font-size: small;">Blockbuster</p> <div style="text-align: center; background-color: #007bff; color: white; padding: 5px; margin-bottom: 10px;"> BLOCKBUSTER CHECK IT OUT! </div> <p style="text-align: center; font-size: x-small;">Start Your Trial</p> <p style="font-size: x-small;">Movies Delivered! Rent Online. Exchange In-Store. Start Your FREE Trial Now!</p> <p style="text-align: center; background-color: #dc3545; color: white; padding: 5px; border-radius: 5px;">Get Your Credit Now</p> </div>	<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p style="text-align: center; font-size: small;">Disney Movies - 3 for \$1.99 Each!</p> <div style="text-align: center; background-color: #007bff; color: white; padding: 5px; margin-bottom: 10px;"> </div> <p style="text-align: center; font-size: x-small;">Sign Up Today!</p> <p style="font-size: x-small;">Join and Get 3 Disney Movies for \$1.99 each! Plus Free Shipping on Initial Order!</p> <p style="text-align: center; background-color: #dc3545; color: white; padding: 5px; border-radius: 5px;">Get Your Credit Now</p> </div>
<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p style="text-align: center; font-size: x-small;">4 Disney books for ONLY .99¢ each!</p> </div>	<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p style="text-align: center; font-size: x-small;">4 Dr. Seuss and his friends books for .99¢ each!</p> </div>	<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p style="text-align: center; font-size: x-small;">\$100 Wal-Mart Voucher!</p> </div>



recently removed 500,000 of them over a one-month period.

The frauds have also copied the Facebook pages of real executives of Publishers Clearing House (PCH), using them to reach out to “friends” and telling them they have won the PCH sweepstakes. PCH has contacted Facebook when it has discovered these bogus profiles, and though they are taken down new ones, quickly pop up. (The same tactics are frequently used on Facebook to offer free government grants that do not have to be repaid. Again, there are fees required to get the money, and there is no real grant).

Similar lottery winner claims appear on [Twitter](#), [Google](#) and [Instagram](#). Scammers on these social media channels frequently impersonate a real person who has won a huge amount in a lottery, and wants to give part of it away to worthy recipients.

Law enforcement tells BBB this type of fraud appears to come mainly from Nigeria and elsewhere in West Africa. Victims are asked to pay through Western Union, MoneyGram, Green Dot and other stored value cards, and gift cards such as iTunes cards.

One victim's story: John

John is a retired teacher from Omaha, Neb., who had gone to Tanzania with a church group. He found it so rewarding that he then went back on his own for a month, helping with a K-7 school and with water testing in a village at the foot of Mount Kilimanjaro. He was very impressed with the local people, and his experience in helping people made a profound impression on him.

When John got home, he was contacted by a friend on Facebook Messenger, who praised his good deeds and asked if he had collected his prize money yet. The friend encouraged him to do so, saying the friend received \$100,000 and noticed John's name on the list as well. His friend sent the information that had the friend's name and John's on the list for winning a random drawing at Facebook. John later learned this was not his friend, but instead a scammer who had copied his friend's Facebook profile.

John found that he needed to contact “Wendy Li Force” through Facebook messenger to collect his winnings.

“Wendy” contacted him, writing: “Congratulations!!! Your profile was selected among our 50 lucky winners. You are entitled to the sum of \$100,000 instantly and it is ready to be claimed now.” After John gave her his contact information, “Wendy” texted him that “Fed X will be on their way to your doorstep. And your money will be delivered to you in the next 24 hours.” She cautioned him that “You are required to keep your money secret until you get it to avoid being robbed on our way to your doorstep.”

She asked that he send \$900 to “Fed X.” He did. Over the next several days, John sent more money to Wendy to cover other fees, such as the cost of the “escort officers” who were delivering the check. Wendy also sent him an “escort certificate,” supposedly from Homeland Security. After that, Wendy claimed that while driving to John's house, they were stopped by a tax agency, which required another payment.

John lost \$9,000. He did not send more money, and of course he never got a prize. He filed a report with BBB and has not heard from the crooks again. John felt bad because he realized how much good the money would have done for orphans in Tanzania. But he says you must simply turn the page and start a new chapter.

Gift card offers

Not all sweepstakes prize offers ask consumers to send money directly to win. Some use these promotions to collect personal information. People will provide a lot of personal information if they think it will help them win something. Consumers should think carefully about what information to share when entering to win a prize drawing or sweepstakes.

The frauds are now running schemes offering smartphones or large gift cards from major retailers on a large scale. This type of fraud initially employed text messages. More recently fraudsters have begun using “pop-ups” that appear on a phone's web browser.

An FTC case illustrates this problem. In [Subscriberbase Holdings](#), the FTC alleged the company sent spam text messages to consumers telling them they had won a \$1,000 gift card from Amazon, Best Buy or Target. The FTC alleged this operation was responsible for 180 million of these text messages.

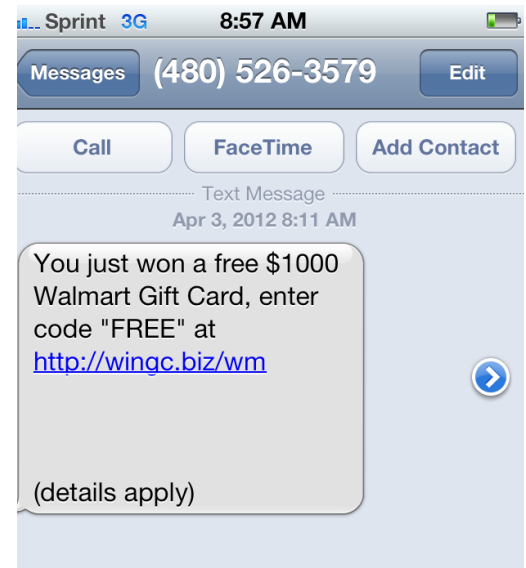
Victims clicked a link to claim their prize. Those who did were instructed to provide their personal information on “where to ship your card.”

Victims were required to fill out page after page of personal information, including data about personal health conditions.

Victims who provided data found they also had to sign up for at least 13 subscriptions or free trial offers for pills or other products, as well as provide credit card numbers.

Those who completed the whole process then learned they had to have three friends complete the process as well. There was no evidence anyone ever received a gift card.

This operation made money by selling the victims' personal information to other companies, including scam robocall operations, and by collecting commissions from



\$1,000 Walmart Gift Card

the companies offering the “free trials.”

This type of fraud has not disappeared. Instead of text messages, this scam now employs pop-up screens on a mobile browser.

Walmart warns about this fraud on its [website](#) and advises people to simply delete the pop-ups. Fraudsters count on enough people going at least partway through the process to make it profitable for them to continue.

C. Sweepstakes prize mailing fraud

Millions of consumers around the world receive deceptive mailings for sweepstakes, supposed psychics, or bogus charities. Fraudulent mailings fall into two categories:

- Consumers receive official looking documents telling the recipient they have won a great deal of money or prizes and need to send some money back in a pre-addressed envelope.
- Consumers receive sweepstakes winning notices that often impersonate Publisher's Clearing House. The notices provide a phone number for the victim to call and talk to a live person to collect their prize. This second category may also include a counterfeit check or money order.

Those who receive a great deal of mail have likely sent money to another scam in the past, and have found their way onto victim, or “sucker,” lists that are sold to other fraud operations; they are at serious risk for many other types of fraud. Relatives and friends can help older consumers avoid becoming fraud victims by educating them, watching their incoming junk mail and helping them identify suspicious items.

Unfortunately, victims rarely complain about this

type of fraud. Victims often send \$20-\$30 each time, over months, and individual losses can mount into the tens of thousands of dollars. In **one FTC case**, the FTC found after bringing suit that only one victim in 1,000 had ever filed a complaint. Moreover, many caregivers or local police do not necessarily understand this fraud, and they may not provide help to repeat victims or assist them in reporting to BBB or law enforcement.

In addition, the names and other information about these victims are then sold to other frauds, such as Jamaican sweepstakes scams, which can devastate elderly victims. The bogus mailing business is truly organized worldwide, and victims collectively are losing hundreds of millions of dollars. Actors in this industry do not seem to be involved in other types of fraud or crime, and they seem to prefer to think of themselves as legitimate mailing businesses. Although there have been impressive law enforcement efforts recently to tackle this type of fraud, it seems unlikely to disappear.

This is a worldwide fraud concentrating on older consumers in most countries around the world. In another FTC case, the fraud was sending its mailings to victims in 155 different countries around the world. Moreover, it is common for different parts of one of these fraud operations to take place in several different countries. Thus, international cooperation has been needed to attack this fraud.

Sweepstakes/lottery fraud process

The FTC's **2013 case against Liam Moran** of Ventura, Calif., may help illustrate how this scam works. Moran sent millions of fake prize notifications through the mail to consumers around the world. The notifications came in envelopes stamped “urgent” or “time sensitive.” They were



personalized with the consumer's name and festooned with PIN and approval numbers, seals, barcodes and contained large-print statements such as "Over TWO MILLION dollars has been reserved for you" and "This document will not be re-issued and is for your use alone to claim eligibility."

Another tells consumers it is "an extraordinary day... [e]specially if you've never ... experienced the opportunity of winning a major lottery or sweepstakes before," and warns that most people "find this news startling at first so take a deep breath."

On the back of these mailings was a disclaimer set in dense fine print that did not make it sufficiently clear the business did not guarantee the receipt of sweepstakes prizes. The fine print suggested entrants would receive a pamphlet giving them lists of sweepstakes they could enter. There was no evidence Moran actually sent these. Even if consumers did receive this mailing, it would be of no practical value.

Consumers were instructed to complete a short form and put a sum, usually \$20-\$30, into an enclosed pre-addressed envelope within a specified 'deadline,' and told not to delay.

The pre-addressed response forms to these mailings are barcoded. This allows the fraudsters to maintain a database of the targets who have responded and to whom they can then send more mailings.

Victims who sent in money never received anything. The pre-addressed envelopes containing the money went to a post office box in Ventura, Calif., not far from Moran's home. Canadian law enforcement had shut down a PO Box he had previously used in British Columbia.

Over a two-year period, Moran sent 3.7 million pieces of mail. He had some of his mail bulk shipped to England, where it was supposed to go into the Royal Mail and then sent around the world. London Metropolitan Police officials detected and seized the mail before it could be sent.

Moran had been involved in deceptive mailings since at least 1995, and in the three years before the FTC shut him down, he had taken in over \$11 million. Much of the money was in foreign currencies, so he had to have it converted to U.S. dollars. Moran eventually **settled with the FTC** and is now banned from this industry.

Sweepstakes/lottery fraud industry supporting actors

Locating and taking action against those operating these frauds can be a challenge. In addition to those operating the fraud, there is a large supporting industry that plays an important role in disguising who is involved and typically receives the money from the victims. These third parties typically do the following work to support the fraud:

- **Writing the mailings.** Note that these

mailings employ carefully crafted wording to avoid saying directly that the victim has won. In addition, the "disclosure" needs to be written in such a way that it can try to deter legal action. These mailings also need to be translated into a variety of different languages.

- **Printing the mailings.** These mailings are often in several colors, and large volumes of them need to be mass printed. In addition, most need to be personalized so that they contain the name of the actual recipient.
- **Maintaining lists of targets.** The frauds need lists of names of people to whom they can send mailings. There are markets, some underground, where the frauds can buy and sell lists of potential victims – and past victims who can be targeted again.
- **Sending the mail.** There is a cost for postage. In addition, the frauds may have the mail shipped to another country and then placed into the mail to disguise the source of this mail.
- **Post Office boxes or mail drops to receive the mail back from victims.** The frauds are never going to have the return mail and accompanying money sent directly to them. Instead they open, or hire others to open, mail drops such as Post Office boxes. These may well not even be in the United States.
- **Opening and sorting the mail from victims.** There is a huge volume of mail coming back to these fraud enterprises, and simply opening it and removing the money can take considerable effort. There are companies known as "caging services" that will perform these duties for the frauds.
- **Handling the money.** Victims often send money in cash, from different currencies if the fraud operates worldwide. In addition, some victims send checks or money orders, which need to be cashed. All of these





funds must then go into some sort of bank account and then transferred to the actual fraud operators. Some caging companies also perform this service.

D. Sweepstakes fraud by phone call

A somewhat different type of fraud uses mail to get recipients to call the scammers to learn about winnings. The mailings provide a phone number for recipients to call, and often include cashier's checks, which recipients are told will cover taxes or other costs associated with receiving the money. Those who call are assured that they have won. They are instructed to deposit the cashier's checks into their bank account and then to withdraw most of the money and send it by Western Union or MoneyGram to some supposed third party. Victims are often told they can keep the rest as an advance on their winnings.

This is a variation on a whole set of frauds that employ fake checks. Often the checks mailed to victims use the names and routing numbers of real companies – but with the company phone number altered so that fraudsters can answer calls.

Under federal banking laws, when a person deposits a check, the bank is required to credit the money to a person's funds quickly, often within 24 hours. Because the bank provides quick access to the funds, the victim concludes the check is good. But the check is counterfeit, and it may take a week or two before the banking system concludes that the check is a fake. When this happens, the bank holds the depositor responsible for the 'bad' check and withdraws the money from the victim's account. Thus the victim has sent their own money to the fraudster, and the bank is generally not liable. More information about such frauds are [available here](#). BBB recently produced an excellent video [explaining how this fraud works](#).

Because such mailings are for illegal activity, the [U.S. Postal Inspection Service actively tries to keep them out](#) of the mail with interdictions at the points where such mail enters the U.S. It is no surprise that some of these frauds also use counterfeit postage. In fiscal year 2017, Postal

Inspectors removed 3,652 such parcels with an estimated postage value of \$266,969 from the mail stream.

Postal inspectors also screen mail to stop counterfeit postal money orders. Last year, [USPIS reported](#) that inspectors interdicted 13,724 counterfeit postal money orders and 550 non-counterfeit postal money orders with a total face value of \$14,157,204.

Because foreign lotteries are illegal, inspectors also directly stop sweepstakes and lottery mail as well. Last year they caught 1,083,903 illegal lottery solicitation letters detailing 4,723 different scams. Those mailings had counterfeit checks with a face value of \$62 billion. Approximately 963 Canadian telephone numbers used in the illegal lottery scam letters were terminated as a result of these interdictions

E. Payment

2015 data shows that 75 percent of the time, money passed going through Western Union and MoneyGram.

Victims take cash to Western Union or MoneyGram and send it on. It is like sending cash; as soon as the money is picked up, the victim has simply lost their money. There are no rights to a refund or chargeback, as there might be if a credit card were used.

Though most financial transactions through their services are legitimate, Western Union and MoneyGram have recognized the problem, especially in Jamaica, and both have taken strong measures in the last couple of years to help prevent fraud. The main legitimate purpose of Western Union and MoneyGram is for family members working in the U.S. to send money back to relatives in their home countries. Most remittances sent from the U.S. to family members in Jamaica are for only \$300 or so. Larger transfers for \$1,000 or more, a common loss for a fraud,

CSN Complaints against Jamaican Companies by Payment Method, 2015

Payment Method	Complaints	Percentages	Amount Paid
Bank Account Debit	42	1.0%	\$201,420
Cash/Cash Advance	135	2.0%	\$2,383,239
Check	153	2.0%	\$2,235,697
Credit Card	67	1.0%	\$257,847
Internet/Mobile	16	0.5%	\$688,051
Money Order	272	4.0%	\$1,591,545
Prepaid Card	236	4.0%	\$2,215,233
Telephone Bill	12	0.5%	\$477
Wire Transfer	685	11.0%	\$4,049,010
Wire Transfer - Moneygram	1722	27.0%	\$4,816,299
Wire Transfer - Western Union	3031	48.0%	\$6,429,746



stand out in the Western Union system.

No legitimate business requires payment by Western Union or MoneyGram. The FTC recently amended the Telemarketing Sales Rule to make it illegal for anyone in a telemarketing transaction to obtain payment by Western Union, MoneyGram or through a stored payment card such as Green Dot. Anyone asking for payment this way in a telephone transaction is violating the law.

MoneyGram settled a case with the FTC in 2011, entering an order requiring it to increase its fraud-prevention efforts. In January 2017, [Western Union settled civil and criminal charges](#) with the FTC and the Justice Department, agreeing to amend its practices to stem the use of its systems for illegal conduct. In addition, Western Union agreed to pay \$586 million to victims who sent money from 2004 to January 2017.

Prepaid cards: Another payment method that has become popular with fraudsters is prepaid cards. In 2014, 26 percent of Jamaican fraud victims paid with prepaid cards. Here is how those work.

A Green Dot card can be used just like a debit card. The cards are registered with Green Dot's computer system. To add money to the card, a consumer buys a MoneyPak card, which is nothing more than a piece of cardboard with a scratch-off number on it. The store adds the money to the Green Dot system, and the consumer scratches off the number and enters it into their online Green Dot account. Green Dot then adds the money to the account electronically. The user can withdraw the money from an ATM machine or purchase goods with the "debit" card.

The fraudsters figured out that they could have someone else provide cash, obtain the MoneyPak card, scratch off the number, and simply read that number over the telephone to the fraudster. This information can be entered into the Green Dot computer system from any location or country.

There are other cards – Vanilla Cards and Reloadit cards are some – available at many retail locations that work the same way. Some of the others also can be reloaded through the Green Dot MoneyPak system.

iTunes cards: Scammers recently began asking people to purchase iTunes gift cards. The numbers from these cards can be read over the phone to the fraudsters. The numbers cannot be used to purchase Apple electronics, but there is a large underground market for these gift cards. No legitimate business takes payment with iTunes or any other gift card.

Cash by mail: As Western Union and MoneyGram have begun taking stronger methods to curtail the use of their systems for fraud, the fraudsters have begun to turn to other methods of getting funds from victims. They tell some to take cash and mail it. Because this is the use of the mail for fraud, the Postal Inspection Service has been working to intercept such mail and stop it from being delivered. When the Postal Inspection Service intercepts such mail they reach out to the sender/victim and return their money.

Bank accounts: Lottery frauds, particularly those from

Jamaica, also have recently begun to use bank accounts. The fraud operations, or their confederates, open bank accounts at major U.S. banks, obtain an ATM card and mail those to the scammers. Victims are told to go to a local bank branch and deposit money into that account. The frauds can then use the ATM cards to withdraw money from those accounts in other countries. Banks close down such accounts when they learn of them, but this tactic is apparently successful. Moreover, the use of a trusted local bank may give these transactions an additional appearance of legitimacy.

Money mules: As Western Union, MoneyGram, and Green Dot have made increased efforts to limit the flow of money directly to the scammers, the frauds there have turned to extensive use of money mules. They have someone else in the U.S. receive the money and then send it on to Jamaica or to a Jamaican gang member living in the U.S. or Canada. While most people are doubtless honest and hard-working, there are some people willing to help launder money for a cut of the proceeds.

In at least one instance a woman from Jamaica flew to Georgia to convince an elderly woman to continue sending money. Vania Lee Allen even impersonated an FBI agent to get the victim to call a co-conspirator in Jamaica in order to keep the fraud going. [Allen was arrested in the U.S. and prosecuted](#). She pleaded guilty and was [sentenced](#) to 40 months in prison.

In addition, the frauds draw repeat or chronic victims into helping them move the money. When the crooks are convinced that the victim has no more money to send, they promise that a third party in the U.S. will send them part of their winnings, at times claiming it is reimbursement for some of the money they have lost. Thus, they use older fraud victims to receive money from other victims and then send the money to Jamaica. In fact, at least one older victim with Parkinson's disease did as asked and [flew to Jamaica with \\$9,000 in cash](#). He was arrested and sent home.

6. What's being done?

Law enforcement

Deceptive mailings: The Justice Department made two worldwide efforts to tackle these deceptive mailings; one in [2016 with Attorney General Loretta Lynch](#) and another with [Attorney General Jeff Sessions in February 2018](#). Here are breakdowns of the [2016 effort](#) and [the 2017 enforcement](#) actions. They include both criminal cases and civil cases seeking injunctions to stop conduct and freeze money for return to victims.

In addition to actions by the Department of Justice, other legal action announced was taken by the FTC, the Iowa and Kansas Attorneys General and by Dutch and Canadian law enforcement. Although a number of different law enforcement agencies took part in this effort, special mention must go to the U.S. Postal Inspection Service, which is responsible for the federal mail fraud laws, and to the International Mass Marketing Fraud



Working Group, originally formed by the Department of Justice with participation from a number of other countries around the world, including the United Kingdom, Netherlands, Nigeria, Canada and Spain.

Collectively, these cases allege fraud losses of over \$250 million. Tens of millions of pieces of mail were sent from these enterprises. Given that victims sent in relatively small amounts of money, such as \$20, it seems plain that there were millions of victims just in the U.S. The various enforcement actions addressed activity taking place in Canada, France, India, the Netherlands, Singapore, Switzerland, Turkey and the U.S.

These efforts included actions against the companies directly operating this fraud, those who wrote the mailings, those that printed and mailed them, and companies that open the mail and deal with the money. They also included cases against those who sold the names of victims.

Telephone Scammers: There have been significant efforts to prosecute in Jamaica, to prosecute Jamaicans and others in the U.S. assisting the fraud, and to extradite Jamaicans to the U.S. to stand trial.

U.S. and Jamaican authorities are working together to fight this fraud. Agencies in both countries have been working together, organizing as Project JOLT (Jamaican Operations Linked to Telemarketing). Project JOLT includes, in part, representatives of the Postal Inspection Service, Homeland Security Investigations (HSI), the FTC, FBI, the Department of Justice and Jamaican law enforcement.

The Postal Inspection Service, FBI and HSI have people stationed full time in Jamaica. In fact, Jamaica is the only place where the Postal Inspection Service has someone posted outside the U.S.

There have now been many prosecutions of those physically in the U.S. working with Jamaican scammers. BBB has identified at least 30 different people that have been prosecuted in the U.S. over the last year or so for involvement in Jamaican lottery fraud. U.S. law enforcement has been working to close off the flow of money from victims to Jamaica.

Extradition from Jamaica In April 2015, Damian Barrett was extradited to the U.S. to stand trial. This was the first extradition from Jamaica for lottery fraud. **Barrett later pleaded guilty.**

The District of North Dakota has successfully extradited 14 people from Jamaica for lottery fraud. All but two have pleaded guilty. One of those extradited was a former policeman. Jamaican law enforcement were cooperative in this effort. Several of these individuals went into hiding but were eventually located by Jamaican law enforcement. Senior officials in the Jamaican government report they would support extradition efforts to the U.S.

The State Department also has warned that hundreds of additional extraditions from Jamaica may be on the way.

Costa Rica enforcement There have been roughly 50 indictments of people involved in Costa Rican lottery fraud over the last few years, many of whom have been

extradited from Costa Rica. Others have been indicted and then arrested when they have traveled outside the country.

Most of these enforcement actions are the work of a unit working with the U.S. Attorney's Office in North Carolina. It includes investigators from the Postal Inspection Service, Homeland Security, the FBI and from the IRS criminal unit with prosecutions handled by the fraud section of the Justice Department's Criminal Division in Washington, D.C. This unit also has received cooperation from the U.S. Embassy in Costa Rica, along with law enforcement in Costa Rica

Foreign lotteries

It is illegal for those in the U.S. to enter foreign lotteries. Organizations sending mailings and making phone calls claiming that someone can win the Canadian, Jamaican, Australian or Spanish "El Gordo" lottery are operating illegally in the U.S.

The FTC has brought cases against Canadian operations that promised people they could invest with others to pool investments in buying Canadian lottery tickets and sharing the winnings. But the FTC contended that most of the money invested was not even used to buy lottery tickets. The FTC found that there were deceptive claims made about the chances of winning. In addition, it is illegal to sell foreign lottery tickets in the U.S.

Lead lists

How do the frauds know whom to contact for their fraud? Like many telemarketers, sweepstakes fraud operations buy lists of names of potential victims. These are known as lead lists. There is a large and legitimate industry which sells names for marketing purposes. Simply do an internet search for "buy telemarketing leads" and hundreds of sellers will appear. Fraudsters also purchase lists, sometimes through back channels. The frauds themselves also sell lists of people who they have previously defrauded. These are known in the fraud industry as "sucker lists." In addition, some frauds use these lists to call and claim they can help consumers recover money lost to a previous fraud - for a fee. These are known as recovery room frauds.

Many of the lists originate from the prize mailing industry. Several lead list sellers involved in the mailing industry have been prosecuted in the last year, in part for their sales of leads to Jamaica, Costa Rica and Israel.

Jamaican officials believe these leads are incredibly valuable. Jamaican law enforcement believes many of the murders there are the result of efforts to steal leads from rival groups.



7. Tips and Recommendations

How can you detect and prevent sweepstakes/lottery fraud? Here are some tips to tell fake sweepstakes and lottery offers from real ones:

- **True lotteries or sweepstakes don't ask for money.** If they want money for taxes, themselves, or a third party, they are most likely crooks.
- **Call the lottery or sweepstakes company directly to see if you won.** Publishers Clearing House (PCH) does have a sweepstakes **but does not call people in advance to tell them they've won.** Report PCH imposters to their hotline at 800-392-4190.
- **Check to see if you won a lottery.** Call the North American Association of State and Provincial Lotteries at 440-361-7962 or your local state lottery agency.
- **Do an internet search of the company, name, or phone number of the person who contacted you**
- **Law enforcement does not call and award prizes.** If you think you have been contacted by law enforcement, verify the identity of the caller and do not send money until you do.
- **Talk to a trusted family member or your bank.** They may be able to help.

What should you do if you believe you have been a victim of sweepstakes/lottery fraud?

File a complaint with:

- **Better Business Bureau.** [Click here](#) to find your local BBB.
- **The Federal Trade Commission (FTC):** ftc.gov; or call 877-FTC-Help.
- **The FBI's Internet Crime Complaint Center:** ic3.gov/complaint/default.aspx
- **The U.S. Postal Inspection Service:** 1-877-876-2455; <https://postalinspectors.uspis.gov>
- **Senate Subcommittee on Aging Fraud hotline:** 1-855-303-9470
- **Western Union:** 1-800-448-1492; <https://www.westernunion.com/us/en/file-complaint.html>
- **MoneyGram:** 1-800-926-9400; <http://global.moneygram.com/nl/en/how-to-report-a-problem>
- **Facebook:** You can report hacked or copied profiles.
- **Green Dot:** 1-866-795-7597; <https://www.greendot.com/greendot/account/contact-us>
- **Canadian Anti Fraud Centre:** Toll free from the US at 1-888-495-8501
- Victims who are seniors or other vulnerable adults may be able to obtain help through Adult Protective Services, which has offices in every state and many counties. Find a local office at www.elderjustice.gov.

Can I stop the mail from coming?

- There may be no single way for victims or their relatives to stop fraudulent mail. If no one responds to the mailings, however, they might stop.
- Some family members have filed a change of

address with the post office so they can receive and screen an elder victim's mail on their behalf.

- Stop catalogs and other advertising mail by contacting the Direct Marketing Association (DMA). DMA members are typically legitimate businesses that would rather avoid the expense of sending mail to someone who does not want it. You can get on a **"do not mail" list**. This service is free on line; it costs \$1 for those who respond to them by mail.
- DMA has a do not mail service specifically for caregivers.

Recommendations

1. Jamaican government should increase its support and fund strong law enforcement to fight lottery fraud.
2. Law enforcement authorities in the U.S. should do more extraditions and prosecutions of fraudsters operating in the U.S.
3. Law enforcement around the world should continue to apply pressure to and prosecute deceptive mailing organizations and end this type of fraudulent mail.
4. It would be useful to have a one-stop telephone number where people can call to find out if they in fact won a lottery or sweepstakes, something like 1-800-Did-I-Win. If such a center had contact with real prize and sweepstakes companies, it could help prevent fraud.
5. Facebook and other social media platforms could make additional efforts to prevent fake profiles from being posted and to actively search for and remove them. Also, these platforms could make it easier for members to contact it about fraud issues, and they should take speedy action against complaints.
6. Western Union, MoneyGram and Green Dot should continue to make efforts to prevent payments to frauds on their systems.
7. More research is needed to understand how fraud succeeds in duping older individuals and what can be done to prevent it.

About the Author

Steve Baker is the former Director of the FTC's Midwest Region where he worked on consumer fraud matters for more than 30 years. He serves on the Board of Directors for the Council of Better Business Bureaus and is BBB's International Investigations Specialist