GIFT CARD PAYMENT SCAMS

BBB reveals why scammers love gift cards

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: MARCH 2021

WHY DO SCAMMERS WANT GIFT CARDS?

Gift cards have become a very large industry, with worldwide sales in the billions. According to the Gift Card Retail Association, they have been the most popular gift for 14 years in a row. A recent AARP survey found that two-thirds of the public intended to buy them for the 2020 holiday season. With more people staying at home, gift cards have become even more popular during the COVID-19 pandemic.

Better Business Bureau (BBB) finds that gift cards have also gained in popularity as a payment method for scammers over the last several years. For scams to be successful, crooks need a way to get money from victims. Using a variety of excuses, such as a threat of immediate arrest, scammers convince victims to buy the gift card as a payment method and ask for the numbers on the back of the cards. This enables scammers to quickly steal the money loaded on the cards.

Gift cards join the list of new methods scammers use to part victims with their money. As noted in a recent update of a BBB study on puppy scams, scammers now often ask victims to pay through Cash App or Zelle. In addition, BBB is beginning to receive reports where victims are asked to insert cash into Bitcoin ATMs, and that payment method is a growing concern.

Providing the numbers from the back of a gift card is just like sending cash. Whether victims give the numbers over the phone or text a photo of the back of the card, they are essentially handing money to scammers, who may quickly drop the funds into foreign bank accounts. It's nearly impossible to get the money back because gift cards do not have the same protections as credit or debit cards. Scammers use this method of payment especially in government impersonation, tech support, and romance scams.

The Federal Trade Commission (FTC) states, "Anyone that demands payment by gift card is always a scammer." In addition, the FTC's Telemarketing Sales Rule (TSR) has extensive provisions governing telemarketing. The TSR does not currently prohibit the use of gift cards in telemarketing but does forbid the use of reloadable cards — such as Green Dot or Vanilla cards that can be used at ATMs — in these transactions. This study explores the differences between types of cards.

This BBB study looks at the scope of fraud involving gift cards as a payment method, the way various cards work, the scammers who exploit them, the efforts to combat the scams and the steps that the industry can take to further tackle this scourge.

HOW BIG IS THE GIFT CARD PAYMENT SCAM PROBLEM?

BBB's Scam Tracker system shows a substantial increase in losses involving payments with gift cards over the last several years. Reported losses nearly tripled between 2017 and 2020. The median loss was $700 in 2020.

YEAR	BBB SCAM TRACKER REPORTS	LOSSES
2017	647	$1,179,563
2018	1,153	$1,780,924
2019	949	$2,083,413
2020	985	$2,953,174

According to a **December 2020 analysis by the Federal Trade Commission (FTC),** "About one in four who lost money to a fraud say they paid with a gift card. In fact, gift cards have topped the list of reported fraud payment methods every year since 2018. During that time, people reported losing a total of nearly $245 million, with a median individual loss of $840."

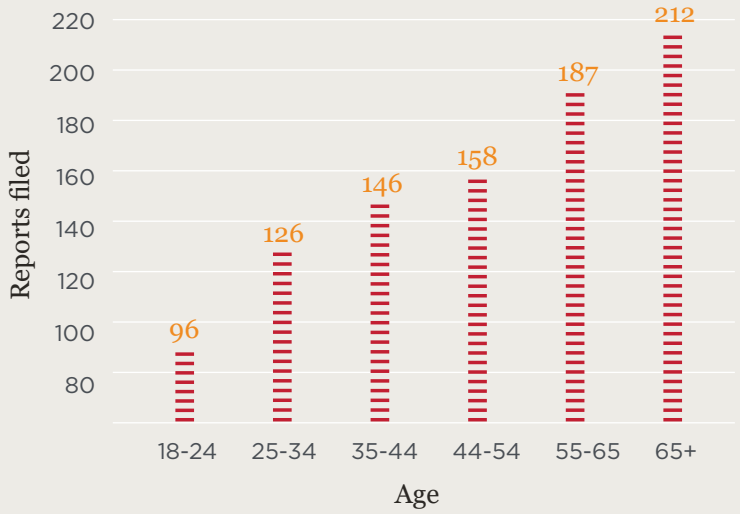
The FTC's statistics exclude reports categorized as online shopping scams and come from consumer complaints directly to the FTC. They do not include any third-party data contributors such as BBB or state Attorneys General.

The Canadian Anti-Fraud Centre (CAFC) has seen gift card payment scam complaints double since 2017.

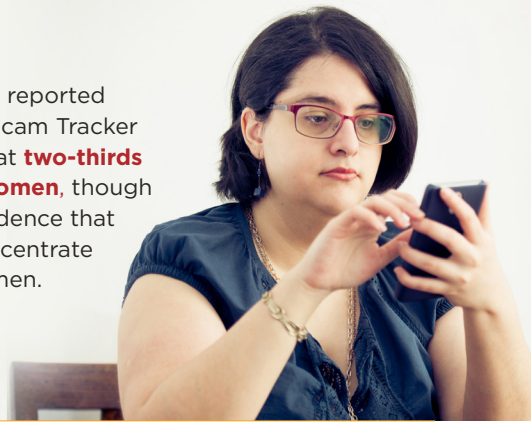
YEAR	CAFC COMPLAINTS	LOSSES
2017	1,222	$2,302,769
2018	2,098	$4,012,392
2019	2,301	$4,218,913
2020	2,702	$3,203,428

WHO IS BUYING THE GIFT CARDS USED IN SCAMS?

2020 BBB Scam Tracker Reports by victim age



BBB Scam Tracker 2020 data show more victims of gift card scams were **over age 65** than for other age groups.



For those who reported their gender, Scam Tracker data shows that **two-thirds (67%) were women**, though there is no evidence that scammers concentrate efforts on women.

WHICH CARDS ARE MOST COMMONLY USED IN SCAMS?

The FTC's 2020 Data Spotlight found, "...Most reported gift and reload card brands are eBay, Google Play, Target, iTunes, and Amazon. Together, these five brands make up approximately 39% of the reports where people indicated they paid a scammer with a gift or reload card."

Canadian regulators state that Steam cards, used for online gaming, are one of the top cards victims are asked to buy in that country.

All of these cards are "closed loop cards," usable only at their own sites or stores. They all contain scratch-off PIN numbers and can be used to make purchases online. Each of these companies has posted warnings about scams and how to avoid being defrauded.

EBay gift cards can only be used at eBay. **EBay warns of gift card scams** and provides some useful examples of emails from scammers detailing the different ways scammers direct victims to make payments.

Amazon gift cards can only be used at Amazon.com. The company states, "No legitimate sale or transaction will require you to pay specifically with gift cards."

Steam Wallet gift cards can only be used to buy Steam video games, in-game items, software, and hardware.

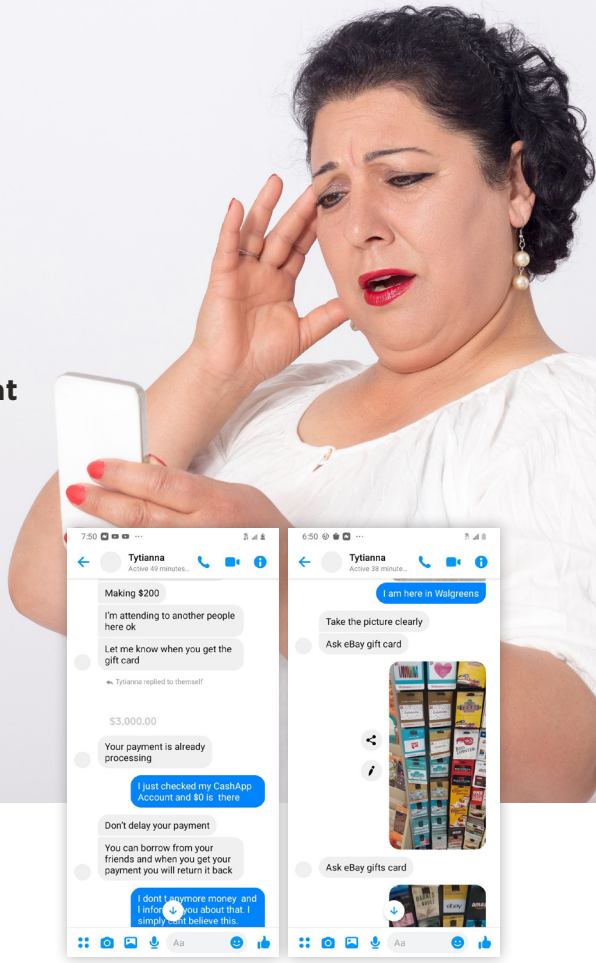
Google Play gift cards can only be used at the Google Play store to buy apps for Android phones, and Google has provided **warnings about scams** using its cards. Google has also partnered with the **National Consumers League to warn** about fraud using their cards.

Target gift cards can be used at a "brick and mortar" store or online. **Target warns about fraud in the use of its cards.**

Apple and iTunes gift cards can be used to buy goods and services from Apple. Apple has warnings about scams **employing its gift cards to buy non-Apple goods.** The company **has recently instructed** its employees to tell those buying Apple gift cards that the cards cannot be used to pay taxes and can only be used at an Apple retail location or at the App Store.

WHY DO PEOPLE FALL FOR GIFT CARD SCAMS?

If victims ask questions about why gift cards are being used for payment, scammers invent a plausible excuse, such as that the government has recently entered a contract with a gift card company to handle transactions.



According to the FTC, "Scammers always have some reason why you need to buy gift cards. They might say you're in serious trouble with the government and must buy 'electronic vouchers' to avoid arrest. Some people say scammers posing as businesses promised special promotional pricing for phone or TV service if they paid for the first three months with a gift card. Others thought they were buying gift cards to evaluate a retailer as a 'secret shopper.'" The reasons vary by scam.

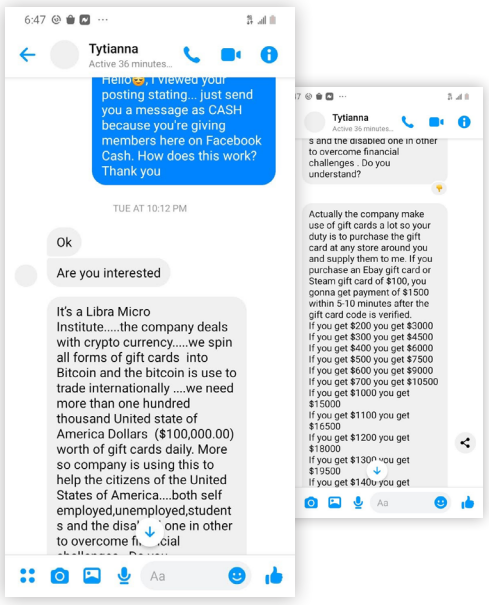
What instructions do gift card scammers give victims on how to buy gift cards?

Scammers typically ask victims to drive to familiar local retailers to buy gift cards, and tell them what kind of gift cards to buy. The scammers frequently stay on the phone with the victims during the entire process, which may take hours and visits to several locations. And they mainly want victims to buy the cards with cash instead of a debit or credit card, which may require an initial stop at the victim's bank.

Fraudsters typically create a sense of urgency that encourages victims to comply with instructions and act quickly. Often victims are scared because they have been threatened with arrest and told that it is illegal to tell anyone else about the situation. Others believe they have won a major prize in a lottery, but they will not receive the money unless they take immediate action.

Victims may be instructed by scammers about how to respond if a teller or cashier asks victims why they are making the purchase. Cashiers at retail locations may want to pay special attention to customers who are continuously on the telephone during the checkout process. That could be a sign that they are receiving instructions from scammers.

It is a good idea for anyone who buys a gift card to keep the receipt. Sometimes the clerk may fail to activate the card correctly. And if a scam is involved, some companies request proof that the victim they are talking with actually purchased the card.



Carolyn lives in the Chicago suburbs and is working toward becoming a real estate agent. In September 2020, she got a Facebook friend request from a woman. "Tytianna" claimed to be a God-fearing mother of two who lived in Florida. Carolyn believed Tytianna was a real person whom she could trust.

A week or so later, Tytianna messaged Carolyn about a worldwide program to help people during COVID. She told Carolyn that any money she provided could be increased. She asked Carolyn to buy a $100 eBay gift card and in return, Carolyn would receive $1,000. Carolyn put this off a week, but she did need the money. So after persistent messages from Tytianna, Carolyn went to Walgreens and bought the eBay gift card. She sent Tytianna photos of the receipt and the numbers on the back of the card. Tytianna said she would send the money to Carolyn via Cash App — but she never did.

The next morning Tytianna contacted Carolyn and asked her to buy another gift card for $100, telling her she would get $2,000. Carolyn recognized that this must be a scam and asked for her money back. She sent several angry messages to Tytianna before blocking her messages. She complained to BBB and reported the scam to her local police department and Facebook. Carolyn never received the promised money.

HOW MANY SCAMMERS ASK FOR GIFT CARDS AS PAYMENT?

The FTC recently did an in-depth examination of loss reports to show which scams were most likely to demand payment with a gift card. Here are their results:

48% of Government Impostor Scams

In this scam, callers impersonate the Internal Revenue Service, the Social Security Administration, or U.S. Immigration and Customs Enforcement (or the Canadian Revenue Agency or Service Canada). They claim that the consumer has done something illegal, and must either pay a "fine" with a gift card or move their money temporarily to a "safe" account by purchasing gift cards. This type of fraud is detailed in the BBB study on government impostor scams.

44% of Family/Friend Impostor Scams

Emergency scams typically takes one of two forms. In one form, victims receive calls supposedly from grandchildren in urgent need of money. The other form involves an email or text from a friend who is supposedly stranded abroad or in trouble, and who needs a short-term "loan" to help them out.

35% of Business Impostor Scams

Often this involves emails or text messages from "the boss" asking an employee to buy gift cards for a seemingly benign purpose (e.g., I want to reward some top performers by surprising them with a gift card). This type of fraud is discussed in the BBB study on business email compromise frauds.

33% of Tech Support Scams

Scammers use popups, robocalls, or other means to convince victims that their computers have serious problems. The scammers get into victim computers remotely, "find" nonexistent problems, and offer to "fix" them for a fee. Read BBB's study on tech support scams.

25% of Romance Scams

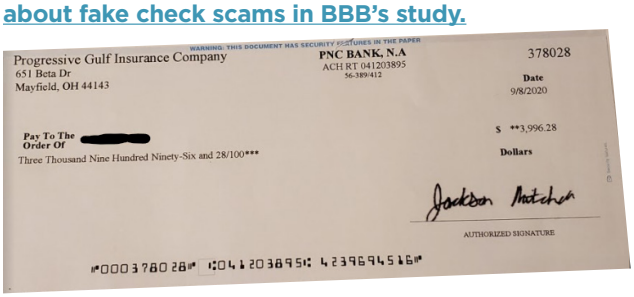
In this scam, victims believe they have found a loving relationship with someone they met online but who cannot meet in person. After building a relationship, the scammer claims an urgent need for money. The BBB describes this devastating scam in its study.

24% of Prize, Sweepstakes and Lottery Scams

In these scams, victims typically get a phone call saying that they have won a large cash prize, often pretending to be from Publishers Clearing House. Victims are always asked to pay a fee in advance, often to cover taxes. No one ever receives the promised money. BBB's study describes how "winners" lose millions through this evolving fraud.

17%
of Fake Check Scams

A variety of scams employ counterfeit checks. Victims are given a counterfeit check, usually a business or cashier's check, are told to deposit it and wait until the money is credited to their account, and then are told to withdraw the proceeds and send money to a supposed third party. Victims do not realize that having the money credited temporarily to their account does NOT mean that the check is valid. When the check bounces, the victim's bank makes the victim repay the amount of the check. **Learn more about fake check scams in BBB's study.**



Teneisha lost her job in Dallas doing quality assurance after the pandemic began. She was looking for work, so she posted her resume on a job board. In October 2020, she got an email offering her a $25.50-per-hour job with a company claiming to be LEO Pharma. She was instructed to interview through Google Hangouts, which she'd never used before. The "interviewer" told her that she would be doing quality assurance, reviewing products as a one-time project that would pay $2,500. She was told that they would send her a check that she needed to deposit so she could pay the company's vendors for a laptop, software and working materials.

Teneisha received a business check in the mail for $3,996.28. She deposited it. A day or two later, she saw that the money was credited to her account, so she believed the check was valid. She was asked to buy Apple gift cards, but she was reluctant to buy them because she was not familiar with them. So they instructed her to get $3,000 in American Express prepaid cards instead. She went to CVS and bought them with her debit card. After she sent photos of the cards and the numbers on the back to the person she had been dealing with, she never heard from them again.

Several days later, her bank told her that the check she had deposited was no good, and the bank assessed fees. She lost $4,046 in total. When she called the real LEO Pharma, they said they had not been dealing with her. They suggested she was likely the victim of a scam and should contact BBB.

OTHER SCAMS THAT NOW USE GIFT CARDS

A **BBB study on online sales of nonexistent cars and other vehicles** found that victims were often asked to pay with gift cards. In addition, **petscams.com** reports that some victims of online sales of nonexistent puppies, kittens, and other pets are now asked to pay with a gift card. **BBB's pet scam study digs deep into how pet scams are evolving.** The **New York Police Department** has also warned that victims of utility scams are being asked to pay with gift cards.

Who are the gift card scammers?

Scam gangs around the world have turned to gift cards as a method of getting money from victims, including:

- Scammers running prize/lottery scams, often from Jamaica
- Business email compromise and romance frauds, often operating out of Nigeria
- Government impostor and tech support fraud operations, typically in India
- Pet scammers, frequently from Cameroon
- Gangs, often in Romania, involved in the sale of nonexistent cars and other vehicles

IS IT LEGAL *to* GET PAYMENTS THROUGH GIFT CARDS?

It is specifically illegal to seek payment with a reloadable card in a telemarketing transaction. The FTC's Telemarketing Sales Rule (TSR) forbids several payment methods in telemarketing transactions in the U.S., including wire transfers (such as through Western Union and MoneyGram), remotely created checks (when victims read their bank account information over the phone and scammers create a check to debit their account) and prohibit use of reloadable cards (such as Green Dot, Vanilla, and many cards that work with the Blackhawk network).

Anyone requesting payment through these methods is violating the law. Canada does not have a similar law, although they are allowed to prosecute those who engage in fraud.

Scammers may not be deterred by the TSR — since they are responsible for the fraud no matter how they obtain the money — but it does provide a clear line so the public knows that anyone asking for payment by these methods is acting illegally and should not be trusted. Even if victims may not know how the scam works, it is important for them to know that anyone who seeks or obtains funds through these prohibited payment methods is violating the law.

In addition, anyone assisting or facilitating telemarketing fraud can be liable for violating the TSR. The FTC has used this assisting and facilitating authority to take legal action against both **Western Union** and **MoneyGram,** asserting that they provided "substantial assistance" while "knowing or consciously avoiding knowing" that they were aiding a scam.

WHAT DO *consumers need to know* ABOUT GIFT CARDS AND HOW THEY WORK?

BBB interviews with victims reveal that while they often know that gift cards exist and can be used, victims may not fully understand how the cards actually work and how they are used by scammers. Similarly, those considering legal or policy changes in response to the increased use of this payment method may benefit from some brief background on the different types of gift cards available, the laws that apply to them, and the protections purchasers may have — if any.

For example, the FTC's TSR prohibits requesting or receiving payment with a reloadable card, but does not currently prohibit payment by gift cards. Therefore, it is important to understand the difference between the types of cards.

The category of "gift card" reflected in victim complaint data to BBB, the

FTC, and the CAFC encompasses a variety of different products, but essentially there are two different types of cards available:

1) open or closed loop cards with a specific value

2) prepaid or reloadable cards that are functionally debit cards and can be used at ATMs.

Consumer Reports has a useful article covering the relative merits of these different kinds of cards.

Gift cards are different from debit cards, which draw money from a pre-existing bank account, or credit cards, which effectively allow users to make loans that need to be repaid by paying the bill, and lack the legal protection these products may provide if a scam is involved.

Gift cards are available at a very wide variety of retail stores across the U.S. and Canada and are typically found in separate display racks. The cards themselves are of no value until activated, so a shoplifter would find them of no use.

The first gift cards began with a magnetic strip, or "mag stripe," on the back. The virtue of these cards is that they can be used in conjunction with the retail Point-of-Sale (POS) computer system to deduct funds when the cards are used and keep track of how much money remains. Many gift cards can also be purchased or used online, though scammers often want people to buy them at a physical store with cash.

Traditional gift cards

There are two kinds of traditional gift cards. First, there are "closed loop cards" that can be used only at specific stores or chains of stores. Second, there are "open loop" cards with a determined amount of value on them which can be used anywhere.

Closed loop gift cards

Most gift cards are closed loop cards. Some closed loop cards are sold for a fixed sum. When the buyer pays for the card at the register, the barcode on the packaging is swiped into the point of sale (POS) system. The card is **activated** and can be used immediately. The magnetic strip contains the card number, which also is typically printed on the back of the card. Other gift cards allow the buyer to decide how much money to place on the card, and again, the POS system records and stores the value remaining on the card.

In some cases, the cards have a PIN that is covered, and the user must scratch off the cover and enter the numbers or code to activate the card. Cards with a PIN are often used to order goods or services online. Most of the cards that are popular with scammers have a PIN. Some cards need to be activated online using the numbers on the back of the card.

A card does not need to be physically "swiped" for it to be used. Anyone with the card number (and activation number or PIN, if there is one) can check balances at a website set up by the retailer. In addition, some cards can be used to buy physical goods at online marketplaces (Amazon and eBay), to play online games (Steam), to buy downloadable music and videos (iTunes), or to buy games and apps for a cellphone (Google Play). They **generally cannot have more money added to them** (there are exceptions, **such as Starbucks**) and cannot be used at ATMs.

Closed loop cards are mainly subject to **state** and **provincial law,** which, as scammers know, currently provides little protection in the event of fraud. Unlike credit or debit cards, there is no ability to reverse the transaction if it is the result of fraud, although when gift cards are purchased with credit cards, victims may be able to challenge the charge with their bank or credit card issuer.

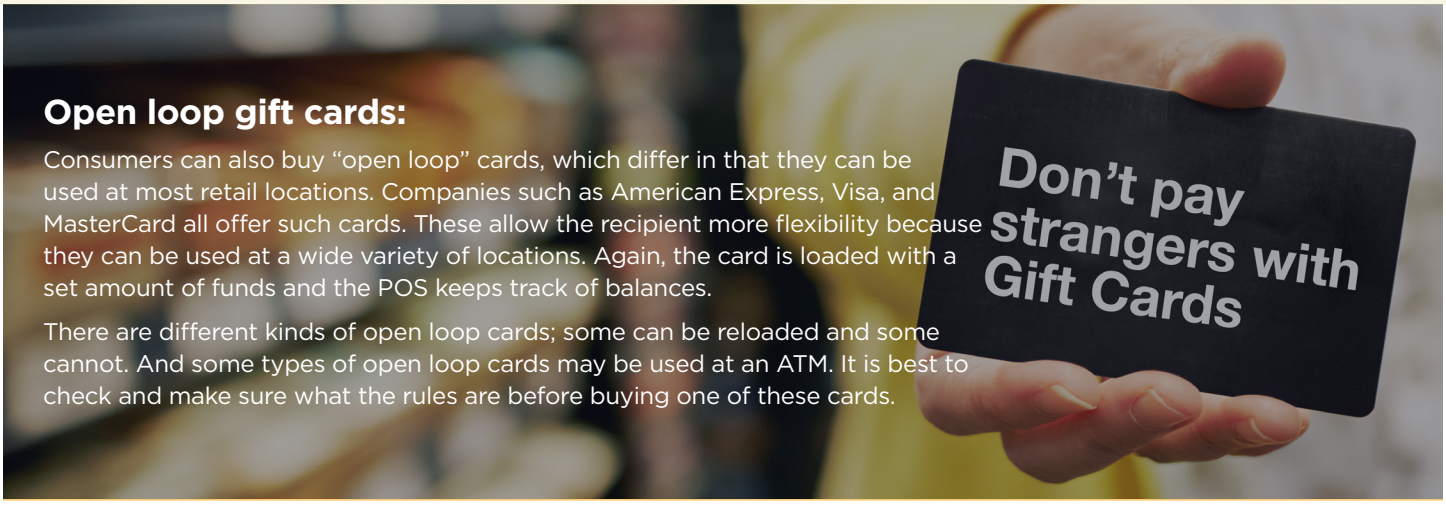
Donna is a retired nurse in Sioux Falls, South Dakota. In March 2020, she received an instant message from a high school "friend." The friend claimed to have received a grant and that her bank said it was real. The friend said she noticed Donna's name on the list of winners and urged Donna to find out more. Donna was skeptical but trusted her friend, so she called "Morris Malani" of Cash Explosion.

Morris explained that this was a government stimulus cash grant provided randomly to people. He told Donna she could get $100,000 that would not need to be repaid. Intending to pay off her mortgage and car debt and donate to charities, Donna bought $550 in Amazon gift cards from Walgreens as instructed -- five $100 gift cards and one $50 gift card. She sent Morris photos of the back of the cards and of the receipts.

When Morris asked for Donna's bank account information to deposit the grant money, Donna refused. Morris said Federal Express could deliver a check within five hours, but since it was Sunday evening, the money would be delivered the next day. On Monday morning, he texted Donna that the money was en route.

But a 3:30 p.m. text message said "dispatch agents" had been stopped by U.S. Customs and Donna needed to pay a fine of $1,450 before they would release the agents. She refused to pay, even though her friend urged her to proceed. Donna realized that government money should not be going through U.S. Customs. When she texted Morris about her concern, he offered to refund $550, which she never received.

A call to Donna's high school friend revealed the friend's Facebook account had been hacked and she had not been involved in this situation. Donna filed a complaint with BBB.



Open loop gift cards:

Consumers can also buy "open loop" cards, which differ in that they can be used at most retail locations. Companies such as American Express, Visa, and MasterCard all offer such cards. These allow the recipient more flexibility because they can be used at a wide variety of locations. Again, the card is loaded with a set amount of funds and the POS keeps track of balances.

There are different kinds of open loop cards; some can be reloaded and some cannot. And some types of open loop cards may be used at an ATM. It is best to check and make sure what the rules are before buying one of these cards.

The federal CARD Act of 2009 generally protects gift cards from expiring and from unexpected fees that would drain the value from them. According to credit.com:

In general, issuers cannot impose a dormancy, inactivity or service fee with respect to a gift certificate, store gift card or general-use prepaid card unless there has been no activity in the previous 12 months, required disclosures (describing fees) have been made, and no more than one fee is charged per month. Also, it is generally illegal to sell or issue a gift certificate, store gift card or general-use prepaid card that is subject to an expiration date unless the expiration date is at least five years away and the terms of expiration are clearly and conspicuously stated.

As a practical matter, few gift cards expire or have fees imposed if they are not used, though it is a good idea to read the language on the back of the card to be sure.

Reloadable cards

Some cards are reloadable and can be used at ATMs, making them popular with scammers. Cards offered through the networks of Green Dot, Blackhawk, and Vanilla can be purchased at retail locations. American Express, Visa, and MasterCard also offer similar products. With these cards, the user must have an online account and can use the card to pay bills electronically. They have a magnetic strip on the back that enables the cards to be used for debit payments or withdrawals at ATMs. Some government agencies also download retirement or Social Security benefits onto this kind of card when people do not have other bank accounts. As noted, the TSR forbids telemarketers from seeking money with reloadable cards.

How do you load more money onto a card? Scam victims often are asked to purchase a "reload card" at gift card racks. These reload products are simply a piece of cardboard with a scratch-off number on them. The victim gives the cashier money to load onto the reload product. The cashier enters that amount into the POS system, and the scammer has the victim scratch off the number and provide it over the phone or by text message. Then the person with the physical card (such as a scammer) enters the number obtained from a victim into an online account. The money is then credited to the account and the card can be used like a debit card or at an ATM to withdraw cash.

In response to large numbers of complaints, **Blackhawk, InComm**, and **Green Dot** testified to the **Senate Aging Committee in 2015** about ways they were combating fraud that used their products. InComm and Green Dot said that they were changing their systems to only allow a reload when the consumer brought in the physical card and swiped it. However, all three companies — Green Dot (**Moneypak**), Blackhawk (**Reloadit**), and InComm (**Vanilla Reload**) — currently sell products to reload cards without having the physical card present.

Prepaid/reloadable cards are subject to a **rule by the Consumer Financial Protection Bureau.** Canada's Federal Consumer Agency (FCA) also has **separate regulations for prepaid (reloadable) cards issued by banks,** such as American Express, MasterCard or Visa. These laws in the U.S. and Canada do not provide much protection for scam victims, since they mainly ban certain fees and require appropriate disclosures.

Cheryl is a therapist living with her family in the Bay Area. In August 2020, she received a phone call from a man claiming to be with the Alameda County Sheriff's Department. The caller ID displayed a local police phone number. The "officer" told her she was in contempt of a federal court order because she failed to respond to a subpoena. He said she had to pay $4,000 in bail to avoid arrest and a much larger criminal fine. The caller also told Cheryl that the court had issued a "gag order," which prohibited her from talking to anyone about this situation. He threatened arrest if she hung up or called anyone. Because she sometimes does make court appearances for her job, she was very concerned that she had made an error and actually was in trouble.

Staying on the phone with her, the caller sent Cheryl to her bank to withdraw cash to pay for three $500 Moneypak cards at CVS and two at Rite Aid, where a clerk asked if she was involved in a scam. The clerk mentioned a similar situation involving a utility company and told her not to give anyone information on the card. But the "officer" was listening from the cell phone and told Cheryl to complete the purchase.

Frightened and suspicious because the caller wanted the numbers before she had finished buying cards, Cheryl switched lines on her phone and called 911 while she was driving to the final location to buy more cards. The police told her it was a scam. Relieved that she had not provided the scammer with the numbers on the back of the cards, she drove to the local police station.

HOW DO SCAMMERS CASH OUT GIFT CARDS?

Once scammers get the numbers from victim's gift cards, how do they actually get the money? Gift cards are generally limited to use in the country where they are purchased, though some cards bought in Canada can be used in the U.S. and some reloadable cards may be used outside the country. Scammers have several different ways to get the money.

• They can use the numbers on the back of the cards to buy physical goods. Because open and closed loop gift cards can only be used in the country where they are purchased, this means that scammers will often use money mules — people who transfer illegally acquired money or goods — to go to stores and buy things like phones or electronic goods that they can then resell at online sites such as eBay or Craigslist.

• Scammers can use gift cards to buy goods sold online at places such as eBay or Amazon and have them shipped to money mules to be resold at online markets or reshipped out of the country.

• Some cards can be used at ATMs. If they are, scammers can simply withdraw cash.

• The numbers from the cards can be resold on sites like Craigslist, eBay, or a variety of other online marketplaces. There are reports that the two most prominent online marketplaces for gift cards were Raise and Cardpool. Cardpool states, however, that it is no longer accepting gift cards. However, there are a variety of others, including gift card granny, cardcash.com, giftcardspread.com, cardbear.com, retailmenot.com, cardkangaroo.com and many others.

• The cards can be exchanged for cryptocurrency. Internet security firm Agari reports that at least one Nigerian BEC fraud gang sells gift cards they get from victims for bitcoin at an online exchange called Paxful. The bitcoin can then be converted into currency and deposited into the bank accounts of fraud gangs. Agari relates that a gift card can be redeemed, converted, and placed in a bank account in Lagos, Nigeria, in less than four hours.

Agari reports, "Paxful recently told the online media outlet CoinDesk that it averaged $21 million a week in transactions in 2018 — up from $8.5 million in 2017. It attributed the growth in part to its user base nearly tripling in Ghana and more than doubling in Nigeria to more than 300,000 accounts. In fact, African users make up nearly 35% of all Paxful accounts." Paxful states that it makes efforts to prevent scammers from using its site.

• A class action filed in federal court against Apple alleges that scammers launder iTunes cards through Apple's online store. The court recently ruled that the allegations were not legally sufficient to find Apple liable but has allowed the plaintiffs to amend their complaint.

Allegations in the court complaint describe how scammers can use the App Store to launder gift cards. A victim buys an iTunes gift card for $500. The retailer reports to Apple that this particular card was sold, that the amount was $500, and notes where and when it was purchased. The retailer does not report any other information from the victim who makes the purchase. The victim provides a scammer with the card number and PIN.

Before the card can be used, the scammer enters the scratch-off PIN into an online Apple account tied to an Apple ID they have obtained from the company. ITunes cards can only be used by someone who has obtained such an ID from Apple. To get an Apple ID, the applicant must also provide Apple with a valid phone number or email address for this ID. Apple also requires that those with Apple IDs provide credit card information or other billing information for these accounts. At this point, Apple knows which Apple ID is associated with the $500 from the card the victim purchased.

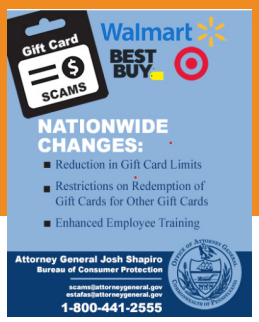
The suit alleges that scammers then redeem these cards through the Apple App Store. So scammers create a useless app, offer it for sale at the App Store, and offer in-app purchases. Apple says it investigates before it lets people sell products at the App Store, and that app developers have to provide Apple with a business name, valid email or phone number, and an account where they can pay the developer that owns the app.

So a scammer with the PIN from the $500 iTunes card enters it on an Apple ID they control. They go to the scam app at the App Store, and make an in-app purchase to "buy" the worthless app with the $500 iTunes card. Apple knows that this purchase has been made for this app, how much was spent, which Apple ID was used to buy it, and also has the information on the gift card that is now redeemed — so they can be sure that the same card is not redeemed more than once. Apple waits 45 days more to pay the scam app developer $350, keeping a 30% commission.

The money is laundered. The lawsuit asserts that there are many complaints to Apple about cards being redeemed at the same place on the App Store, and Apple should be able to see patterns. And since Apple knows which Apple ID was used, they can also track which app the gift card was used for the purchase.

WHAT GIFT CARD SCAM RED FLAGS SHOULD CASHIERS WATCH OUT FOR?

Clerks and cashiers often see people come into their locations buying gift cards under suspicious circumstances. For example, scammers try to keep victims on the line during the entire process of buying cards from local retailers, so someone who is continuously on the phone should be a red flag. Industry members also suggest in their training for clerks that it is unlikely that older victims would be buying gift cards used mainly for online gaming.



Many retailers train their front line personnel on scam activity. CVS pharmacy says that when a gift card is swiped, a warning about gift card scams will appear on the panel so the purchaser will see it before they can complete the payment for a gift card. Walmart and CVS encourage employees to decline the sale if the circumstances are suspicious. Walmart even recognizes and rewards employees who take action to prevent such fraud.

Intervention in the store selling gift cards may be an effective tactic to limit this type of fraud. A report by **FINRA, co-authored by BBB,** found that 51% of people were able to avoid a scam because of intervention from a bank teller, store employee, or other third party.

Janet is 86 and lives near Springfield, Missouri. Just after Halloween in 2020, a woman called, claiming to be from Apple. She said Janet's iCloud data storage had been compromised. Since Janet was an iCloud user, she was very concerned. The caller transferred her to another man, who said in order to protect her data, Janet needed to buy gift cards and she would be reimbursed later.

Over the next two days, Janet purchased 29 $500 gift cards. At Walgreens and Target, she bought Target cards, and at Walmart, which doesn't sell Target cards, she bought Walmart gift cards. The caller told her to scratch off the numbers on the back of the card, take a photo with her phone and send him the photos. At least one clerk asked her if this was legitimate, but she'd been told to explain that the gift cards were presents for grandchildren.

Altogether, Janet lost $14,500. Angry and sad, she changed all of her passwords and credit cards, a process which took nearly a month.

WHO IS COMBATING GIFT CARD FRAUD?

Law enforcement and BBB are making efforts to fight gift card fraud. These measures include not only arrests and prosecutions of the money mules that receive and launder victim money, but also steps to work with gift card companies and retailers to help prevent this type of fraud.

BBB efforts to warn of gift card fraud. In December 2020, **BBB released a tips article on avoiding gift card scams** and a **warning about Cardpool, LLC**, due to a large number of complaints about the Texas-based online gift card marketplace for buying and selling gift cards.

State attorney general/retailer voluntary efforts. In 2018, the Attorneys General of Pennsylvania and New York reached an agreement with Walmart, Target and Best Buy to make changes in their gift card policies. The three voluntarily agreed to engage in enhanced training for their employees, restrict using their gift cards to purchase iTunes, Google Play or Steam cards, and reduce limits on the maximum value of cards and on the total amount of cards that can be purchased during one transaction.

In November 2020, the Arizona Attorney General's office announced an agreement with CVS pharmacy to place a sign warning of gift card scams in its Arizona stores stating, "Gift cards CANNOT be used to pay ANY government agencies." CVS told BBB that it posts warnings about gift card scams at the sales racks for cards at most of its locations nationwide.

The FTC has created tools and materials for use by industry and law enforcement partners that include graphics in English and Spanish for warnings on gift card display racks and tips for cashiers. These are part of an ongoing FTC campaign to fight gift card scams, which also includes both articles and blog posts that encourage people to report possible scams to the gift card companies themselves. Contact information for cards most often involved in scams is found at ftc.gov/giftcards.

Government agencies in both the U.S. and Canada tell BBB that prosecuting government impostor scammers, who increasingly ask victims for gift cards, has been a priority for law enforcement. For example, many Indian nationals have been living in the U.S. and Canada, sometimes illegally, while working directly with scam call centers in India that impersonate government agencies such as the IRS or Social Security Administration or pretend to be with Apple or Microsoft offering to "fix" supposed issues with a computer. Many of these scammers received and laundered money from victims.

- The U.S. Treasury Inspector General for Tax Administration (TIGTA) tells BBB 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 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.
- The Royal Canadian Mounted Police in Canada has prosecuted those handling the money for impostor frauds, including scammers in the Toronto area and in British Columbia.
- In December 2020, Los Angeles police arrested a woman running a "secret shopper" scam. She sent victims counterfeit money orders to deposit into their bank accounts and then had them buy gift cards. Victims of this type of scam believe that they have been hired to evaluate the customer service of a business.
- In 2018, a scientist working at the University of Wisconsin was convicted of laundering $300,000. The Milwaukee Journal Sentinel reports that he was receiving gift card numbers from scammers working in India, and that he used those cards to buy iTunes cards, which he sold in China as part of an international scam.
- In November 2020, criminal charges were filed in federal court in Virginia against a Chinese national who was involved in a conspiracy to launder over $1 million in gift cards obtained from victims of IRS and similar scams.
- Also in November 2020, a federal court in Tampa, Florida sentenced a man to more than five years in prison for laundering gift cards illegally obtained by scammers through an online redemption site he operated.
- In a recent DOJ case against an India-based robocall provider, the government alleges that these calls often impersonated the IRS or Social Security Administration and directed victims to purchase gift cards.

WHAT RED FLAGS AND TIPS HELP CONSUMERS AVOID GIFT CARD PAYMENT SCAMS?

Government agencies requesting payment. No government agency ever requests money through gift cards.

Statements that buying gift cards is a safe way to make a payment. Providing the numbers for a gift card is like sending cash, and the money is rarely recoverable.

Keep the receipt when buying a gift card. Keep the physical card as well. These may help prove that the card was paid for and activated if problems arise later.

Inspect the card carefully before buying it to be sure it has not been tampered with. Some scammers open the card to get the numbers on the back so that they can take the money when the card is later activated.

WHERE TO REPORT A GIFT CARD PAYMENT SCAM?

Victims should immediately notify the organization that issued the card as soon as they realize they have bought gift cards and provided the numbers to scammers, or have purchased gift cards with no balance on them. There is typically a customer service number on the back of the card.

The FTC provides phone numbers and other contact information for Apple (which owns iTunes), Google, Steam, MoneyPak and eBay. These can be useful, because victims sometimes say they have difficulty in reaching a live person to report issues. Here is a summary of numbers to call if you have been a victim:

- **Amazon:** (888) 280-4331
- **Ebay:** (866) 305-3229
- **Google Play:** (855) 466-4438
- **iTunes:** (800) 275-2273
- **Steam:** report online at help.steampowered.com
- **MoneyPak:** (866) 795-7969

ALSO FILE COMPLAINTS WITH:

- **Better Business Bureau** - file a complaint with your local BBB if you lost money or report a scam online at BBB.org/scamtracker.
- **Federal Trade Commission (FTC)** - file a complaint online at ReportFraud.ftc.gov or call 877-FTC-Help.
- **Internet Crime Complaint Center (IC3)** - file a complaint online at ic3.gov/complaint.
- **Consumer Financial Protection Agency** – file a complaint online at consumerfinance.gov/complaint or call (855) 411-2372.
- **Canadian Anti Fraud Centre** - file a report online at antifraudcentre-centreantifraude.ca or call 1-888-495-8501.
- **Canadian Financial Consumer Agency** to file a report online about prepaid or reloadable cards in Canada.

BBB RECOMMENDATIONS *to* COMBAT GIFT CARD PAYMENT FRAUD

• **The FTC should consider amending the Telemarketing Sales Rule to prohibit payment with gift cards.**

• The industry should continue to educate the public about the potential pitfalls of gift cards by:

- Including warnings directly on the cards
- Providing warnings on gift card display racks
- Training and educating front line tellers and cashiers
- Including a warning on screen at the point-of-sale where a victim can read it before completing the transaction

• **The industry should consider:**

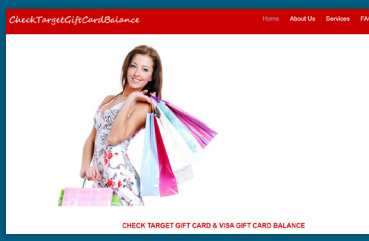
- Additional efforts to limit large dollar volume gift cards and how many can be purchased in one day
- Prohibiting the ability to purchase gift cards with other gift cards
- Imposing a waiting period between when cards are purchased and when they can be used, at least for online purchases. Once the immediate pressure from the scammer is relieved, victims often recognize it is a scam and thus, with a bit more time, could try to stop the transaction.
- Mining their data on gift card fraud to look for patterns and share that information with appropriate law enforcement
- Tracking the speed and location of card redemption. This data may help spot patterns of fraud.
- Making it a practice to provide refunds to victims who realize they are dealing with a scam after purchasing gifts cards and therefore don't give scammers the numbers from the back of the card.

• **The industry and enforcers in the U.S. and Canada should consider holding an in-person conference with relevant partners to examine common issues and understanding of the mechanics of card markets and ways to limit or prevent fraud.**

THEFT OF GIFT CARD NUMBERS

At times, thieves also obtain the money from a gift card before the recipient can use it, even if a victim has not provided the numbers on the back to a scammer or anyone else. An AARP survey from December 2020 found that "over a third (36%) say they have given or received a gift card with no balance on it." It is possible at times that the cashier failed to authorize the gift card properly. But there are other possible ways to steal money from gift cards.

• Many retailers have websites where you can log in, enter the numbers on the card, and check the balance to see how much remains. But some scammers have set up sites that impersonate those of actual retailers. When the victim enters the gift card numbers on these bogus sites, the crooks simply steal the numbers and redeem the money. When the victim tries to use the card, they find that there is no money on it. Industry members try hard to identify and shut down bogus sites, and **BBB has warned about this type of scam.**



> ***Greg*** *is a therapist in St. Louis. In December 2019, he received a Target gift card as a present. The card did not say what the value was, so he did an internet search for a site to give him the balance. At the top of the search results he found checktargetgiftcardbalance.com. The site seemed legitimate and professional-looking. Greg entered the numbers from the back of the card, but no balance appeared.*
>
> *He became worried, and called Target. They explained that this was a scam site with no connection to Target. They told him his money was gone. He urges others to be very careful when looking for sites to check balances on gift cards.*

• Crooks may simply obtain the numbers from the backs of gift cards that have not been sold, and periodically check those numbers at the retailer's website. They can use "brute force" attacks that electronically enter many numbers, one at a time, until they find a card that has since been sold and activated and has available funds on it. They can then use the money on the card. **An article in Wired details the gift card hacking problem.**

The industry has developed several responses to this problem.

• They have tried to design packaging so that the numbers on the card cannot be viewed until the card is given to the cashier to activate it.

• Gift card balance sites now often employ CAPTCHA technology, which requires action by the consumer such as retyping a code that appears. This stops many automated attacks.

• InComm voids all cards where the balance is checked on a card before it has been activated.


BBB