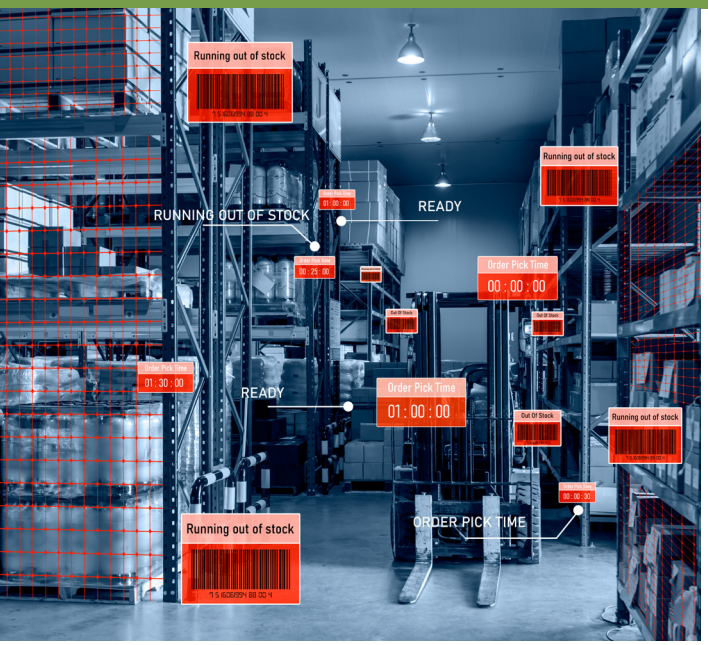
THEFT ON A MASSIVE SCALE: ONLINE SHOPPING FRAUD AND THE ROLE OF SOCIAL MEDIA

A BBB® study finds pandemic and global supply chain crises, along with lax social commerce shopping platforms, opens the door for scammers in China to steal from desperate online shoppers.

BETTER BUSINESS BUREAU®
INTERNATIONAL INVESTIGATIONS INITIATIVE

ISSUED: DECEMBER 2021

ONLINE SHOPPING RANKS HIGHEST AMONG THE TYPES OF INDUSTRY COMPLAINTS REGISTERED WITH BETTER BUSINESS BUREAU® (BBB®) AND FRAUD REPORTS TO BBB SCAM TRACKER LAST YEAR.



"THE VAST MAJORITY OF THIS SCAM ACTIVITY IS BEING CARRIED OUT BY GANGS OPERATING FROM CHINA."

JORIJ ABRAHAM
GENERAL MANAGER
SCAMADVISER.COM

Concerned consumers filed a class action lawsuit against Facebook in August that "...seeks to put an end to Facebook's policy of actively soliciting, encouraging, and assisting scammers it knows, or should know, are using its platform to defraud Facebook users with deceptive ads, and compel Facebook to either compensate Facebook users for their losses or disgorge the billions of dollars in profits it has unjustly earned from such misconduct."

Some fraudsters hinder the ability of people to get their money back by using payment methods with little or no safeguards. If consumers use credit cards or PayPal to buy items online, they may receive a refund if they challenge fraudulent purchases. Many people, however, are not aware of this protection.

Online shopping fraud has been growing for several years, but dramatically increased during the pandemic, according to BBB research. A BBB survey found 29% of people shopped online before COVID, increasing to 37% by the end of 2020. With many stores closed and people staying at home, online shopping increased. But even with fewer lockdowns in 2021, consumers continue to shop online.

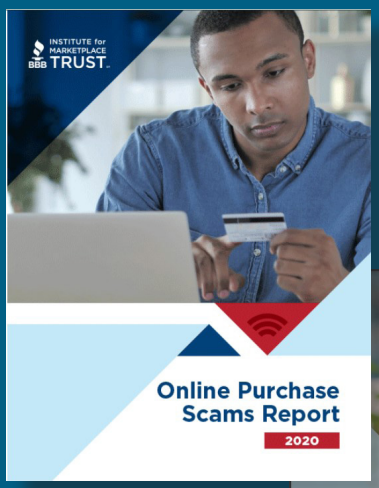
With consumers increasingly worried about supply chain disruptions and forecasts for record-breaking online spending for the 2021 holiday season, it is especially important for online shoppers to know how to protect themselves from deceptive advertising and online scams that may trick them into purchasing non-existent merchandise.

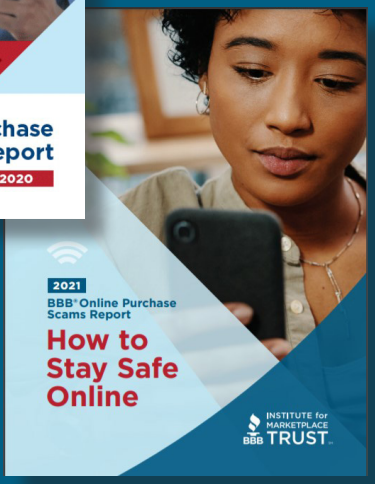
Consumers report online fraud ranging from sales of non-existent vehicles, pets and products to counterfeit goods to costly free trial offers.

The largest group of BBB Scam Tracker reports -- 40% of the total -- involve victims of online ads found on Facebook and Instagram. Consumers tell BBB that Facebook and Instagram are often not helpful in addressing violations of their own policies when consumers receive nothing at all, counterfeit goods, or items that were inferior to what was advertised and purchased. These encounters often take place after seeing enticing social media ads placed by operations in China.

While many legitimate companies based in China sell goods to the U.S. and Canada, this study focuses on goods sold online where victims receive nothing at all, counterfeit items or something quite different from advertised.

This study builds on the 2020 and 2021 Online Purchase Scams Reports from the BBB Institute for Marketplace Trust (BBB Institute) and takes a closer look at:





- How common is online shopping fraud?
- What kinds of fraud are involved in online shopping?
- What makes online purchase fraud work?
- How do scammers exploit payment systems?
- Who is behind online shopping fraud?
- How to avoid this fraud?
- What is being done to fight online shopping fraud?
- What more can be done to protect consumers?
- Where to complain if goods do not arrive or are not as advertised?

How common is online shopping fraud?

For the past five years, online purchases of goods have comprised the largest number of reports to BBB Scam Tracker and been deemed by BBB Institute to be the riskiest scam in 2020. Over the last two years, reports from victims have skyrocketed.

In 2015, online shopping fraud accounted for 13% of all Scam Tracker reports with a monetary loss. By 2021, 64% of all Scam Tracker reports with a monetary loss involved online shopping issues. Complaints directed to the Federal Trade Commission (FTC) and reported losses more than doubled over the last two years and are on pace to quadruple to $394 million. This is not just a U.S. phenomenon. Losses reported the Canadian Anti-Fraud Centre (CAFC) tripled in 2020.

FTC and BBB Scam Tracker data reflect trends rather than the total amount of this fraud. The FTC previously has found fewer than 10% of fraud victims report it to BBB or law enforcement, suggesting the problem is much larger than these numbers reflect.

BBB SCAM TRACKER ONLINE PURCHASES*

YEAR	REPORTS	LOSSES
2019	9,050	$4,228,592
2020	17,942	$6,732,550
2021 (Jan-Sep)	12,699	$6,337,447
2021 (Projected)	16,892	$8,499,292

*These statistics do not include complaint data found in BBB Business Profiles at BBB.org.

Online shopping has more BBB "F"-rated companies than any other type of business (TOB).

BBB data shows the TOBs that comprise electronic shopping produced 106,326 complaints in 2020, up 40% from 2019, and in 2021 are on a pace that may equal or exceed this total. Of those 2020 complainants, thousands mentioned China, Facebook and Instagram in the complaint narratives.

Unlike the FTC and CAFC, BBB Scam Tracker has a separate category for counterfeit goods. In 2020, BBB received 1,396 BBB Scam Tracker reports and those are rising as well. They are on pace to increase to 1,524 in 2021.

FTC ONLINE SHOPPING

YEAR	COMPLAINTS	LOSSES
2019	177,537	$103,538,830
2020	365,101	$250,800,000
2021 (Jan-Sep)	307,280	$295,400,000
2021 (Projected)	409,705	$393,866,000

CAFC UNDELIVERED MERCHANDISE

YEAR	COMPLAINTS	LOSSES
2019	3,368	$4,360,448
2020	6,249	$14,221,943

For 2020, the CAFC said 1,314 of those complainants reported seeing the product on social media.

What kinds of fraud are involved in online shopping?

Most online fraud reports examined involve a response to online ads on Facebook and Instagram. After placing an order, victims either receive nothing or get items that are either counterfeit or dramatically different from those promised. For example, the CAFC's Barry Elliott reports he has seen accounts of people buying a cordless drill online but only receiving a screwdriver from China.

A victim told BBB she ordered a rattan sofa for her patio but received a burlap bag from China months later.

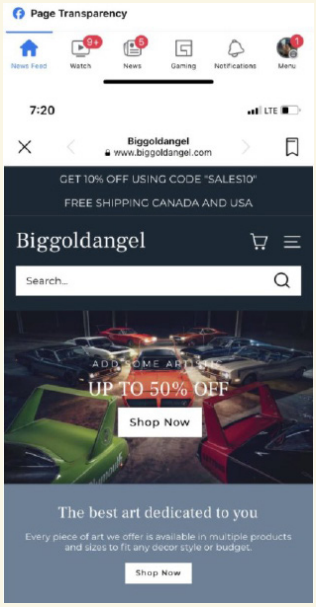
Scammers often take photos or other elements from legitimate businesses, post them on Facebook and Instagram and take online orders at websites they create. These tactics can result in lost sales and a flood of complaints to honest businesses from angry victims who locate them after being scammed. The victims do not realize that their money went to the scammers who posted the advertisement. In addition, many businesses report trying to get fake ads taken down by Facebook and Instagram takes many hours of extra work and is a large burden.

John lives in Dallas and sells art at his online site amazingartexpo.com. He has seen a massive increase in fraud with sales of his art online. This really became a problem for him in June 2021. Scammers were cloning -- making copies of photos -- of the art on his website. He believes the scammers have significantly cut into his business.

The scammers set up bogus Facebook pages and then ran advertisements. He says many of these ads lead to websites that contain the same 11-digit international telephone number instead of a 10-digit domestic U.S. number. Nevertheless, Facebook will not take down these obviously related ads, but instead forces him to challenge the ads one at a time. The art is copyrighted, which makes it easier to challenge scam ads.

He placed orders for the scam copies and several times received nothing. But when he did receive an order, he got low quality prints. He had a tough time getting a refund with PayPal.

He has been trying hard to combat this fraud and initially spent hours each week just fighting the scammers. He has also challenged counterfeit sales of his products on Amazon and Etsy.



A Facebook ad and comment from John about a business he claims is involved in unethical practices.

Many counterfeit items are sold over the internet. Scammers claim to be selling trademarked or copyrighted goods, but if they send anything, it is a fake replica. The items often are produced in China by the same scam gangs that sell other goods deceptively. This is a huge issue for those selling legitimate brand name goods. For more on the massive worldwide problem of counterfeit goods and medicines, see the BBB study on counterfeit goods scams.

The Department of Homeland Security recently observed: "American consumers shopping on e-commerce platforms and online third-party marketplaces now face a significant risk of purchasing counterfeit or pirated goods." It also states that actors such as payment processors, social media websites and online marketplaces "aid, abet or assist" these transactions.

The other reports to BBB primarily fall into three categories, each of which has been the subject of previous BBB studies.

Pet scams

These account for 35% of BBB Scam Tracker reports about online shopping in 2021. As the BBB has reported, those have more than doubled over the course of the pandemic with more people staying at home and finding it a suitable time to add a pet to the family. For example, BBB received 117 reports of pet scams in June 2019, but in June 2020, those had increased to 320. Scammers take money from victims, but no pets are delivered. BBB received 4000 complaints about pet scams in 2020. For more information about pet scams and how they work, visit bbb.org/all/petscams.

Vehicles

One of the top sources of online shopping complaints are fraudulent sales of cars, boats, RV's and other vehicles. Scammers steal photos of those items from elsewhere on the internet, post them for sale and ask interested buyers to send money to a supposed third party for payment and shipping. These scams often claim to be associated with eBay, which has a buyer protection program to safeguard sales on its platform. Victims never receive the vehicles. Craigslist now charges to post advertising for vehicles. Scammers now post many ads on Facebook Marketplace, which has eclipsed Craigslist as a source of classified ads, according to an article in ProPublica. For an in-depth look at vehicle vendor scams and how they work, see BBB's study on vehicle vendor scams at BBB.org/scamstudies.

Free trial offers

Many BBB Scam Tracker reports involve health/nutrition offers using bogus "free trials" of weight loss products, erectile dysfunction products or more recently, CBD products. Despite law enforcement efforts, reports to BBB Scam Tracker continue to go up. Note that only a small fraction of victims of this type of scam report to BBB or law enforcement. Read BBB's study on free trial offers at BBB.org/scamstudies.

What makes online purchase fraud work?

Those shopping online can find goods by doing an internet search, by clicking an online ad on social media, or by shopping at an online platform such as Amazon. The BBB survey of those who reported online purchase scams to BBB Scam Tracker found that the top online platforms on which they looked for products were:

- **32%** Google
- **28%** Facebook
- **8%** Instagram
- **5%** Specific Websites

This survey found that 64% of respondents were actively searching for a product when they lost money, 21% were passively looking and 15% were not looking at all.

Sponsored links

A BBB study found that victims first encountered the ads where they placed orders on Google 32% of the time. One of the features of search engines is that paid advertisers' sponsored links will appear at the top of the search results page. Images can be advertisements as well, again appearing at the top of search results and leading shoppers to scam websites. Scammers often pay for these sponsored links.

Feeling safe on sites like Amazon

Counterfeit goods are common even on sites like Amazon.com. Because Amazon allows third-party sellers to advertise on its site and ship themselves, you still need to be careful. Over half the goods sold by Amazon are by third parties. Amazon collects payments and then reimburses the third parties. There are reports that Amazon gets 15% of sales by these third-party sellers. In a CBS interview announcing these efforts, Amazon conceded that counterfeiting is a problem on its site. According to CBS, "the company caught 3 billion suspicious listings last year before buyers even saw them but can't say how many counterfeits actually made it onto the site."

The role of Facebook and Instagram in online shopping fraud

A large number of BBB online shopping reports can be traced back to Facebook and its subsidiary Instagram. BBB found that victims who were not actively looking for a product, but lost money in the transaction, began with Facebook or Instagram 70% of the time.

This is consistent with a study of complaints to the FTC. The FTC data spotlight from October 2020 found about one of every four online shopping complaints mentioned issues beginning on social media and Facebook and Instagram account for 94% of complaints where victims got nothing and a social media platform was involved. In looking at data from the first half of 2020, 43,391 people (23%) reported to the FTC that the problem started on social media. For the 9,832 who ordered goods that never arrived, victims said the transactions started on social media, with 7,502 of those specifically noting the use of Facebook or Instagram (94% of those that identified a specific platform).

The International Trademark Association (INTA) has warned about social media. Many counterfeit online goods are sold through ads on Facebook and Instagram, which share the same ad network.

Christian lives in Chicago, where he is a flight attendant. He saw a video on his Facebook feed that advertised sand art tables for a great price of $30, which he surmises appeared in his feed because of his previous searches on kinetic art. He went to the site, sylviaharris.com, and placed an order for two tables using his credit card. He did not receive an email receipt or other communication from the company. When the items did not arrive, he tried to call the company but the phone number provided did not work.

He also reached out to the Facebook page of the person who advertised the tables. He posted comments on the Facebook page and was blocked from the page. Christian contacted Facebook dozens of times about this fraud, and they responded that the video did not violate their policies. The ad remained running for several months. Facebook simply stopped responding to him. He complained to BBB, called his credit card company and had the charges removed.

RIGHT: The sylviaharris.com site in November 2021, which is not how it looked when Christian visited the site earlier. New, closed and frequently changing websites could be red flags for fraud.

Facebook and Instagram as attractive locations for scammers' advertisements

Facebook is the biggest social network worldwide. It has roughly 2.91 billion active users. For many, Facebook is a comfortable place to stay connected with family and friends. Therefore, the ads that appear in Facebook feeds also may feel safe.

In reality, the ads that appear are targeted to users. After making an online purchase at one site, ads for similar goods often appear on other sites visited. Crooks understand how Facebook targets shoppers and have developed strategies to reach those likely to be interested in buying their bogus products.

Fraudsters steal photos and copy websites of honest retailers, offer goods for sale, take payment and either ship nothing or send inferior knockoffs. They can quickly form corporations, put up a page on Facebook, buy advertising space and then advertise on Facebook feeds. Victims who click on an ad are taken to a website developed by the scammer where they can place an order. If an ad or website is taken down, scammers can immediately replace it with a new one. These ads have long been the bane of brand name companies selling trademarked goods such as sunglasses, designer handbags and running shoes. For example, it has been reported that 25% of luxury goods sold through Facebook advertising are fakes.

But the problem today goes far beyond the risk that someone will get counterfeit sunglasses. Now almost anything can be sold online. This is especially threatening for small businesses trying to market their products online. Sales can rapidly disappear to crooked sites, not only depriving honest businesses of sales but also resulting in a flood of complaints directed to the real company when victims are ripped off.

Suzanne teaches second grade in Santa Rosa, California. In June 2021, she saw a rattan sofa on clearance for $30 on Instagram. She says the ad was very professional and thought the item would look great on her patio, so she used a credit card to place an order. The sofa had not arrived by August, so she emailed the company and they sent her a tracking number. She was confused when she received a burlap pillowcase in the mail from China. She did not immediately connect this with her couch order until the shipment tracking system said her order had arrived.

When Suzanne emailed the company in China, they insisted she return the pillowcase to get a refund. Realizing that shipping would cost nearly as much as the product, she refused. The "company" eventually offered her a choice between a 70% refund or return of the goods. Frustrated, she complained to the BBB and plans to challenge the charge on her credit card.

Dear customer,
Thank you so much for your patience.

It is a pity that we have not yet been able to provide you with a satisfactory solution!
We do not have a return label, and the options mentioned in the previous email are the best options we can provide. If you still do not accept it, we will have to ask you to return the package. However, you need to pay the shipping cost of the return, which will cost you about $20. According to our experience, the return time may last about 1 month. According to our company's return policy, we cannot refund until we receive the package, please understand. For your benefit, we recommend that you accept a 70% refund. If you still insist on returning the goods, please return to the following address:

Consignee: Xu Shangwei
Zip code: 518101
Address: 2B, 6th Floor, Jinchi Logistics Park, Xingwei Community, Fuyong Street, Baoan District, Shenzhen

Reminder:
1. Please indicate the order number and email address on the package so that we can refund you after receiving the returned package.
2. Please pack it properly to avoid damage during transportation, otherwise we will not be able to refund in full.
3. Please provide the tracking number to help us track the package.

An email Suzanne received from the company and a photo of the pillowcase she received instead of the couch.

Much of online fraud originates in China. Though general user access to Facebook is blocked in China, companies there spend billions on advertising. While many shoppers knowingly buy goods from businesses in China, some shoppers who believed they were buying from a U.S. or Canadian company felt deceived when goods arrive in the mail from China – and especially when they received poor imitations of what was ordered. Laws against deceptive practices offer protection if a U.S. company is involved, but there may be little recourse against advertisers located in China.

Cindy is an artist in Nebraska who has an online store where she cuts scenes in vintage hand saws. Beginning in May 2021, scammers began making inferior copies of her saws, using pictures from her website to advertise on Facebook. Victims who bought these, often as Father's Day gifts, received scam copies that are neither metal nor wood and are about the size of a TV remote control.

She has spent hundreds of hours since then fighting these scammers. In addition to Facebook, scammers now market the counterfeit handsaw art on Etsy and Amazon. She reports that it has been a challenge to understand what can be done. She cannot reach a live person on Facebook. And she found hundreds of ads on Facebook that were all clearly connected. But she had to challenge every one of the Facebook ads separately, despite the common ties between them.

The fake website looked legitimate, using real reviews from her site, actual photos and videos of her.

Eventually, a scammer contacted and spoke with her directly from China. He offered to market her saws. He claimed that it is not a crime to steal designs in China, and no one cares. He said that in two weeks, he had already sold 3,000 units in their first run of bogus versions of her saws. He said that his only job was to find unique art that would be interesting to shoppers, to copy photos from those websites so his company could sell cheap knockoffs. This man claimed 100 other employees in his building, most of them young men, were doing the same thing.

Vintage hand saws from Cindy and a notice she posted on her website to help customers discern her website from the fake.

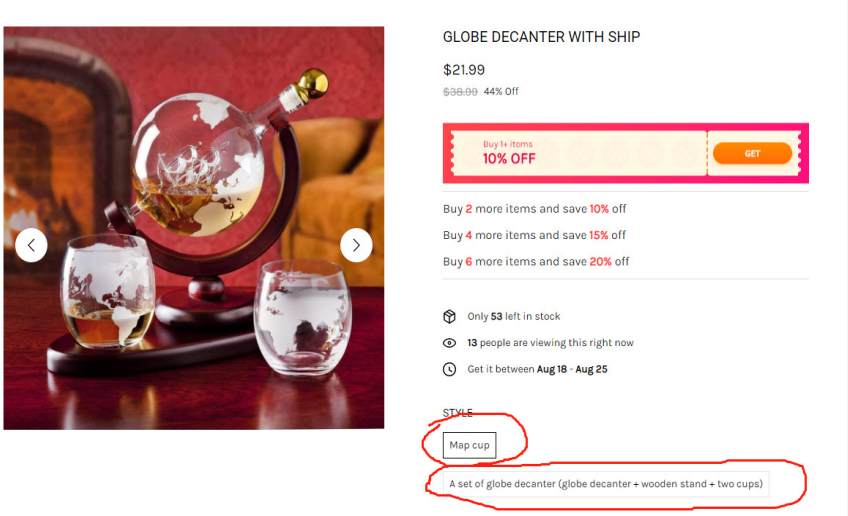
According to a Buzzfeed news article:

A previous internal study of thousands of ads placed by Chinese clients found that nearly 30% violated at least one Facebook policy. This was uncovered as part of the regular ad measurement work performed by Facebook's policy team. The violations included selling products that were never delivered, financial scams, shoddy health products and categories such as weapons, tobacco and sexual sales, according to an internal report seen by BuzzFeed News.

The same article suggests that Facebook intentionally ignores these issues. Problems with China-based advertisers are well known among the social network's employees and contractors, said a person with knowledge of Facebook ads enforcement. "We're not told in the exact words, but [the idea is to] look the other way. It is 'Oh, that's just China being China.' It is what it is. We want China revenue," they said. Similar conclusions have been reached elsewhere. This is not just a U.S. phenomenon. Similar problems have been reported in both the U.K. and Germany.

Many victims and small businesses believe that Facebook and Instagram can do more to prevent this widespread fraud. A class action was recently filed in a U.S. federal court against Facebook, contending that it is complicit in fraudulent sales and fails to abide by its own policies in addressing them.

Valerie lives in Republic, Missouri. She and her husband collect nautical items. Her father served in the Coast Guard. While looking at Facebook she saw an ad for globe decanter with a ship, a wooden stand and two map cups. She decided to buy it as a present for her husband for $29. The site was cyrodir.com. She paid with her credit card. But she only received one cup, though the ad plainly shows this as a set. She contacted the company to complain and was told that she had only ordered one cup. They refused to give her a refund, so she contacted BBB.



Valerie thought she ordered the full decanter set but only received one glass.

These problems occur even though Facebook has announced a variety of policies in its terms of service and community standards that ban advertising which "contain deceptive, false, or misleading claims like those relating to the effectiveness or characteristics of a product or service." In addition, Facebook policies prohibit advertisers from using "tactics intended to circumvent our ad review process or other enforcement systems."

According to Marissa Hadland, who assists with a Facebook group called Facebook Ad Scambusters, victims or small businesses state that they have a grim time getting Facebook to process complaints about ads and Facebook pages that use photos or other information stolen from legitimate businesses and are slow to remove such ads. New ads pop up with the same content and have obvious ties to the one removed, such as the same phone number. It is a frustrating process, she says. She told BBB she believes there are huge internal economic incentives to bring in advertising revenue and that this results in a culture at Facebook that is very reluctant to take effective action against fraudulent advertising. She reports that those who can show they have a copyright on their goods have more success in challenging ads that use their brands.

Casper is in Northern Ontario, where he and his partner Sadie are artists who have developed a series of zombie garden gnomes, 15-16 inches tall in solid cast drystone, that they sell on their website. In April 2021, scam sites using photos of their products began appearing on Shopify sites tied to Facebook ads, Amazon, AliExpress and Etsy. Shoppers who ordered from these sites received six-inch tall plastic replicas shipped from China.

Casper and Sadie say this has devastated their business. They are trying hard to fight these scams but say it is nearly a full-time job just trying to get the sites and ads taken down. They also have heard from victims who are upset, though they are not responsible for the scam sales. Because these are seasonal products, they fear that they will see a real resurgence by scammers exploiting the Halloween and Christmas seasons.

ABOVE: Zombie Gnomes website graphic.
CENTER: An original 15-16" Zombie Gnome.
RIGHT: A 6" plastic counterfeit gnome.

How do online scammers exploit payment systems?

The BBB Institute's study of online purchases in 2020 found that of those who lost money, 35% paid with a credit card; 23% paid with PayPal; debit cards were used by 20%; Zelle payment apps were reported 7% of the time, and prepaid cards 3% of the time.

Zelle
THIS IS HOW MONEY MOVES®

A review of BBB complaints involving payment through Zelle showed that almost all of those were by pet scams. People should never pay for an online purchase using Zelle. There is no protection when a scammer is involved and no way to recover funds.

It is unusual for scammers to seek payment through credit cards. That is because credit card companies keep a reserve of funds to cover chargeback requests from victims. A 1% chargeback rate is high for those holding merchant accounts, and the companies can assess fines or terminate the accounts. The banks that support the system have strong incentives to avoid losing money to scammers.

Researchers at NYU closely examined sales of counterfeit goods, however, and found that they are almost always paid for with a credit card. Therefore, the bogus websites selling these goods must have access to the credit card and banking system. The research shows almost all of these transactions are handled by a small number of banks in China. The NYU study looks at how credit card payments are processed for counterfeit goods. Over two years, they purchased 424 branded products.

All of the goods were drop-shipped from China and were of poor quality. They concluded that the criminal gangs that produce counterfeit goods outsource fulfillment and payment processing.

PayPal

Online scammers are increasingly requesting payment through PayPal. PayPal has a buyer protection program designed to safeguard transactions so it seems secure. Users do not receive a monthly bill from PayPal. The system instead links to victims' bank accounts and credit or debit cards. Nonetheless, victims reporting to BBB often cite difficulties getting a refund through PayPal when they receive goods that are very different from those that they ordered, and news stories report similar experiences. Several sources report that it is more difficult to get refunds through PayPal and suggest that its customer service personnel may simply not be trained adequately on these issues. They also state that it is more effective to talk to an actual customer service person at PayPal than it is to use its online complaint system. Use caution if doing an internet search for PayPal's customer service number as that has been a source of scams; instead, go to PayPal's website directly and connect that way. Victims who realize they have been scammed first try to contact the operation from which they made the purchase. This can be a difficult and frustrating effort. A BBB survey found that 62% of victims reported that they tried to contact the seller more than three times. Even scam websites that claim to have a return and refund program rarely honor them. It can be difficult to reach a customer service person. Instead of a refund, victims are often offered discounts on future purchases. Sometimes the company asks people to be patient and claims that the goods will arrive.

Credit card companies and PayPal have policies that offer refunds if goods are counterfeit or sold fraudulently. Those who don't receive what they ordered — nothing, counterfeit goods or inferior items — should call the customer service number on the back of their card to ask for a refund, a process known as a chargeback. Credit card companies have anti-fraud policies. Consumers can find the policies online for Visa, MasterCard, Discover or PayPal.

Many people are not aware that they can dispute charges, and do not ask for a refund. In one study of free trial offer scams, BBB found that 42% did not request a charge back on their credit card. If shoppers don't receive their orders, they often have success in getting money back if payment was made by credit card, debit card or through PayPal.

Victims should act quickly to dispute charges with credit card companies. They typically have 120 days (four months) from the date they receive the goods OR from when they learn that they were counterfeit. Those with Visa cards have a maximum of 540 days (18 months) from the original transaction. PayPal gives victims 180 days (six months).

Familiar with the dispute processes used by credit card issuers and PayPal operations, scammers have tried to develop a variety of methods to defeat them.

Shipping costs. Scammers may ask victims to return the items before they can receive a refund. But the cost of shipping the items back to China often exceeds what they paid for the items.

Destroying counterfeit goods. In the case of counterfeit goods, the credit card companies and PayPal no longer require that goods be returned, instead asking victims to simply destroy them. If the seller wants the goods back, they can provide a prepaid return label.

Proving fraud. Credit card companies and PayPal may request proof of fraud. It helps if victims requesting a chargeback show that they were promised something different from the item received. The website address, screenshots of the item ordered and received or a printed ad might be enough to obtain a chargeback.

Running out the clock for claims. If scammers can engage with victims and delay the process long enough, people give up or wait too long to file a claim within the time limit set by the credit card companies.

Supplying bogus tracking numbers. Some scam companies send victims bogus tracking numbers. In one study, BBB found that 59% of those surveyed reported that they received tracking data; of those 54% said it was fake. Scammers have used this to claim that goods were delivered even those they were not. After a BBB report on this issue, PayPal announced that this issue has been resolved.

Some victims who have filed complaints about PayPal claim that the company told them to return the goods to the seller to get a refund, but PayPal tells BBB that this is not the case, stating:

You can learn more about PayPal's Protection Program here. Under the Selling & Accepting Payments section of our User Agreement, if the claim was that the item received was Significantly Not as Described and related to an item you sold that is counterfeit, you will be required to provide a full refund to the buyer and you may not receive the item back. Also, disputes must be opened within 180 days of the payment date. Information on this can be found in the User Agreement with other information about Purchase Protection. You can find more about Shopify here: https://help.shopify.com/en/manual/payments/paypal

Victims in Canada have help with refunds

Canadian victims have an easy method of getting a chargeback. When victims contact a Canadian bank that issued the credit or debit card (or PayPal in Canada) and want to dispute a charge because the goods are counterfeit, never delivered, or are different from those ordered, the bank will refer victims to the Canadian Antifraud Centre (CAFC), which operates Operation Chargeback.

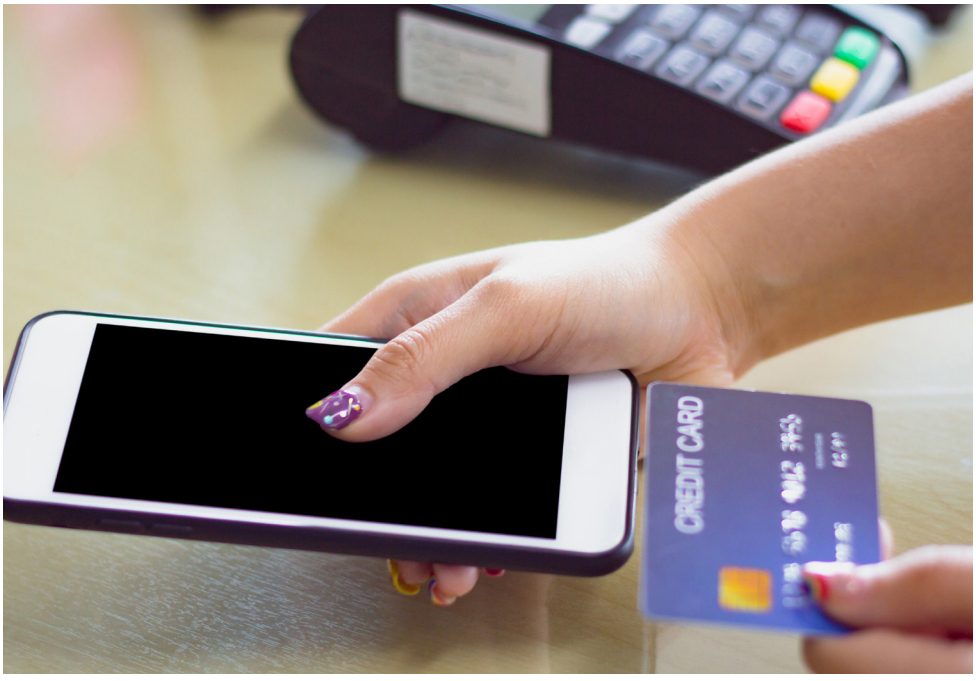
For counterfeit goods, the CAFC identifies the website where the victim purchased the counterfeit in question and contacts the brand — that is, the trademark holder — to see if the site is by an authorized seller. If it is not, the brand notifies the CAFC. The CAFC then provides this information to the victim in an email, and the victim can then provide that email as proof to their bank and get a chargeback. The CAFC also informs victims that they do not need to return the counterfeit goods; rather, they ask people to destroy them. Ebay and PayPal similarly say that they do not require that victims return counterfeit goods.

The CAFC also deals regularly with bank referrals in which the victim receives something different from what they ordered. They ask for photos of the item received, and the webpage of the product they ordered, and respond to the bank that a chargeback is in order. The CAFC recommends that if the seller wants the goods returned, the seller should pay for that by sending a prepaid mailing label.

Last year, the CAFC was able to help more than 6,000 victims. Over the last five years, the CAFC has used this quick and easy process to get chargebacks for tens of thousands of people and more than $14.7 million in refunds. They have identified more than 36,000 websites selling counterfeit goods. There is no program like this in the United States. Through this work, the CAFC also has been able to gather data on 18,000 merchant accounts used to accept payment for counterfeit goods. Those selling these goods must have a merchant account from a bank that allows them to accept credit card payment. The CAFC says almost all of the counterfeit merchant accounts are linked to four state-run banks in China. In addition, the information on websites and merchant accounts that the CAFC obtained is useful to law enforcers and credit card processors.

Who is behind online shopping fraud?

As noted in earlier BBB studies, pet scams are primarily operated by scam gangs from Cameroon. Vehicle scams have been traced to gangs from Romania. Free Trial offer scams seem to be operated by people in the U.S. and Canada. Counterfeit goods operations, as well as those who sell goods online that are not delivered or that are significantly different from those described, have been tracked to China.



What is being done to fight online shopping fraud?

Role of the Better Business Bureau

BBB fights fraud by accrediting trustworthy businesses, identifying fraudsters and their activities, collecting reports from victims and sharing them with law enforcement, and issuing news warnings about scams to help educate the public.

Consumers can conduct a free search to check out a business or website by going to BBB.org. BBB notes customer complaints and how they are resolved, in addition to customer reviews about their experiences with the business.

BBB Accredited Businesses can display the BBB seal on their website, so shoppers may want to look for that as a way of deciding if they are dealing with a reputable business. The BBB seal is trademarked and can only be used by BBB Accredited Businesses that agree to follow BBB's standards of conduct. Clicking on a legitimate seal will take the viewer to the business' BBB Business Profile. If the link is not live, the seal may be fake. BBB finds hundreds of cases every month where there is unauthorized use of its seal. If companies do not respond to BBB's request to remove the seal, BBB notifies website host, and in most cases, the seal is removed.

BBB Scam Tracker collects reports from scam victims or people who have spotted a scam. It has categories specifically for online shopping and counterfeit goods. BBB Scam Tracker sends reports about online shopping and other scams to the FTC's Consumer Sentinel database.

BBB has issued warnings about a home product company selling online and another selling canvas prints for Mother's Day. BBB has warned consumers about fake tracking codes being used in online shopping scams.

Applicable law & enforcement

Although there are laws against deceptive practices those are difficult to enforce against scammers operating outside the U.S. and Canada, especially when they are in China. Typically, actions have been limited to those physically present in the U.S. and Canada and those who work with or help scammers.

For decades, remotely ordered goods have been subject to the FTC's Mail, Internet, or Telephone Order Merchandise Rule, familiarly known as the Mail Order Rule. The Rule applies to goods but not services. Internet sales are covered directly. It was originally adopted in response to problems with catalog companies where goods were often delayed. For example, some businesses would take orders — and customer funds — and then delay shipping them until they had accumulated enough orders and money to pay their own supplier. After paying in full, consumers would end up waiting many months for their products to arrive.

The Rule's solution is to require that goods be shipped when promised, or if no shipping date is provided, within 30 days. If sellers cannot ship within 30 days, they must get consumer's consent to a delay. If they cannot get this consent, they must refund the consumer.

The FTC is authorized to seek civil penalties for Rule violations. At times, state attorneys general have treated violation of FTC Rules as per se violations of their own state versions of the FTC Act.

Canada

Canada does not have a national rule. Instead, this is a subject of provincial law. Under Ontario law, goods must be delivered (not shipped) within 30 days of the promised delivery date or you can ask for a refund. However, it appears that if you do not return the product, you lose the right to seek a refund. The same provisions apply in British Columbia.

In addition, the FTC or the Competition Bureau (or States and provinces) could address deceptive claims about products, such as shipping products different from those advertised. Claims that a business is in the U.S. when it in fact is not would likely be a deceptive claim that the FTC could challenge, because it could mislead people about the degree of protection they have available to them. Criminal charges can be brought against sellers that defraud the public.

Intellectual property issues, including copyright, trademark infringement and theft of trade secrets, are priorities for the U.S. government. In Canada, these issues are handled by the Canadian Border Services Agency.

In 2020, the most recent year for which data is available, U.S. customs agencies seized $1.3 billion in counterfeit goods. They also arrested 203 individuals and secured 98 convictions. More than half of the goods seized came from the People's Republic of China.

Unfortunately, there are few prosecutions of those in China who are responsible for taking money from consumers through deceptive advertising. Although China exercises great control over its people, there is little to show that the government there is interested in addressing this fraud, apart from some actions against copyright violations.

What more can be done to protect consumers?

- Facebook and other social media platforms should do more to enforce its policies for third-party sellers.
- BBB urges credit card payment processors to put more effort into combating those who provide merchant accounts to sellers who engage in fraud.
- U.S. consumers would benefit from a program to help counterfeit victims with chargebacks like the one operated in Canada by the CAFC. Such a program may help identify crooked credit card merchant accounts, bogus websites, and points of origin for counterfeit goods.
- More regulatory oversight is needed regarding companies that use websites to market products from China but deliver nothing, counterfeit goods or items not as advertised.

How to avoid this fraud?

Check out the website before making a purchase:

- **Use BBB.org to check a business' rating and accreditation status. Some crooks may copy the BBB seal. If it is real, clicking on the seal will lead to the company's BBB profile.**
- **Scamadviser.com can often tell you how long a website has been in operation. Scammers create and close websites regularly, so a site that has only been operating for a short time could raise red flags.**
- **Do an internet search with the company name and the word "scam." This may locate other complaints about the site.**

Search for contact information:

- **Use caution if the site does not have a U.S. or Canadian phone number or uses a Gmail or Yahoo business email address.**
- **Look for the company's physical address.**

Keep a record of what you ordered:

- **Make a note of the website where you ordered goods.**
- **Take a screenshot of the item ordered in case the website disappears or you receive an item that differs from what was advertised.**

Scrutinize reviews:

- **Scammers frequently post positive reviews on their websites, either copied from honest sites or created by scammers.**
- **One resource to check reviews is at BBB.org.**
- **Some review websites claim to be independent but are funded by scammers.**
- **Look at the bad reviews first. These are more likely to be real and can help identify scams.**

Pay by credit card:

- **Credit cards often provide more protection against fraud than other payment methods.**
- **Use a third-party payer such as PayPal.**

Where to complain if goods do not arrive or are not as advertised

Report online shopping fraud to:

Better Business Bureau - File a complaint at BBB.org or report a scam at BBB.org/scamtracker.

Federal Trade Commission (FTC) - File a complaint at reportfraud.ftc.gov or call 877-FTC-Help.

National Intellectual Property Rights Coordination Center - Report intellectual property and counterfeiting violations to iprcenter.gov/referral/view.

Internet Crime Complaint Center (IC3) - File a complaint at ic3.gov/complaint.

Canadian Anti-Fraud Centre - File a report at antifraudcentre-centreantifraude.ca or call 1-888-495-8501.

Facebook – Report ads that violate Facebook's policies by clicking the * next to an ad to go to facebook.com/business/help.**

Instagram - Report copyright infringement or other policy violations at help.instagram.com.

Amazon - Report suspicious activities and webpages at amazon.com.

Google - Report scams at google.com.

PayPal - Call PayPal at (888) 221-1161 to speak with a live person instead of using its automated system if you receive an item that is not as advertised.

Your credit card company - Call the phone number on the back of the credit card to report the fraud and request your money back.

About BBB

BBB is a nonprofit organization that sets and upholds high standards for fair and honest business behavior. Most BBB services to consumers are free of charge. BBB provides objective advice, free BBB Business Profiles on more than 5.3 million companies, 11,000 charity reviews, dispute resolution services, alerts and educational information on topics affecting marketplace trust.

BBB's mission is to be the leader in advancing marketplace trust. It accomplishes this by:

- **Setting standards for marketplace trust**
- **Encouraging and supporting best practices by engaging with and educating consumers and businesses**
- **Celebrating marketplace role models**
- **Calling out and addressing substandard marketplace behavior**
- **Creating a community of trustworthy businesses and charities**

Acknowledgements
This study was a joint project of Better Business Bureaus of Chicago, Dallas, Omaha, San Francisco and St. Louis. Contributions include data from BBB Scam Tracker, BBB Institute for Marketplace Trust, IABBB and various regulatory agencies.

BBB International Investigations Initiative contact information
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

By C. Steven Baker, BBB International Investigations Specialist stbaker@bbbinc.org

Find more information about this study and other BBB scam studies at BBB.org/scamstudies.


BBB