NOFRAUD

2024 Fraud Trends: A Guide to eCommerce Threats & How to Mitigate Risk

Get in touch with a Fraud Expert. 888-773-3669 sales@nofraud.com nofraud.com

Contents

Mission Critical: Do Fraud Detection Tools Make a Difference?

In a recent study by the Merchant Risk Council (MRC), more than 1,v000 eCommerce shops were surveyed to understand how successful merchants have been at leveraging fraud management tools to mitigate and thwart fraud threats over the past year. Results showed that the percentage of eCommerce revenue lost to fraud globally, order rejection and fraud rates on domestic orders, and the share of eCommerce orders that led to fraud-related chargebacks all declined significantly. While the impact of fraud has dipped, the amount merchants have spent on managing payment fraud has remained consistent over the past three years — which has been about 10% of their annual revenue.

While the top 10 trending fraud types remained consistent, where they ranked within the list changed, with phishing and reshipping scams seeing the most significant increases.

	2021 Rank	2022 Rank	2023 Rank	Global % Experiencing (2023)
Phishing / pharming / whaling	3	1	1	**43% ↑**
First-Party Misuse (i.e., friendly / chargeback fraud)	1	4	2 🟢	34%
Card Testing	2	2	3 🔴	33%
Identity theft	4	3	4 🔴	33%
Coupon / discount / refund abuse	5	7	5 🟢	30%
Account takeover	7	5	6 🔴	27%
Loyalty fraud	6	6	7 🔴	22%
Affiliate fraud	8	8	8	22%
Re-shipping	12	11	9 🟢	**20% ↑**
Botnets	10	9	10 🔴	19%
Triangulation schemes	9	10	11 🔴	17%

🟢 **Increased Ranking** 🔴 **Decreased Ranking** ↑ **Sig. Higher vs. 2022**

Interestingly, surveyed participants who identified as members of the Merchant Risk Council detected higher levels of specific fraud types compared to their non-member counterparts, which begs the question: Does this group have more fraud detection tools in place that enable them to identify and register a larger share of attacks that impact their business than non-members?

	% Non-Members Experiencing	% MRC Members Experiencing
Phishing / pharming / whaling	42%	54%
First-Party Misuse (i.e., friendly / chargeback fraud)	29%	**91%** ↑
Card Testing	29%	**85%** ↑
Identity theft	31%	**50%** ↑
Coupon / discount / refund abuse	27%	**57%** ↑
Account takeover	23%	**83%** ↑
Loyalty fraud	22%	26%
Affiliate fraud	23%	20% ↑
Re-shipping	18%	**48%** ↑
Botnets	16%	**57%** ↑
Triangulation schemes	14%	**57%**

↑ **Sig. Higher for MRC Members** ↓ **Sig. Lower for MRC Members**

It's unlikely that MRC members are actually experiencing more attacks than non-members. These differences suggest fraud detection tools are mission critical to understanding which fraud threats are really posing a risk to your business. This guide digs into the top fraud trends and highlights how eCommerce businesses can identify risks that compromise their shop's success.

Phishing: Gaining Unauthorized Access for Wide-Ranging Schemes

In an era where digital transactions are the norm, phishing has emerged as a predominant threat, with a staggering statistic from the FBI's Internet Crime Complaint Center indicating that phishing incidents nearly doubled in frequency from 2019 to 2020, leading to billions in losses worldwide. And most recently, merchants reported phishing as the number one threat to their business. This sharp rise underscores the critical need for awareness and robust defense mechanisms against phishing tactics in the eCommerce sector.

What is Phishing?

Phishing is a cybercrime in which targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to trick individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. Both merchants and consumers are susceptible to phishing. Phishers will use social engineering tactics that exploit human psychology to gain unauthorized access to accounts. Cybercriminals use social engineering tactics because it is usually easier to exploit people's natural inclination to trust than to discover ways to hack software. It is one of the most subtle yet powerful ways cyber attackers seek to gather confidential information, as it often relies on human error rather than vulnerabilities in software and operating systems.

How Phishing Happens

Deceptive emails

The most common phishing tactic involves sending emails that mimic legitimate communications from well-known brands, enticing recipients to click on malicious links or attachments.

Spoofed websites

Fraudsters create fake websites that resemble legitimate eCommerce platforms. Unsuspecting users enter their login credentials or payment information, which goes straight to the attackers.

Social media scams

Phishing attempts may also occur via social media, where fraudsters use direct messages or fake ads to trick shoppers into visiting phishing sites — fraudulent copies of a legitimate website — or disclosing personal information.

Smishing (SMS phishing)

Phishers will send text messages, posing as a store representative or shipping carrier, that prompt unsuspecting shoppers to provide sensitive information or download malware.

Spear phishing

Targeted attacks aimed at specific individuals or companies, often using personal information to make the scam more convincing.

Vishing (voice phishing)

Phone calls to deceive people into surrendering personal information.

A RECENT CASE OF VISHING

The Chaotic and Cinematic MGM Casino Hack

Dive into the gripping story of the MGM casino hack — a cyber heist that reads like a thriller but had real consequences for thousands. Find out how a sophisticated social engineering attack led to the breach of one of the biggest names in the entertainment industry, compromising sensitive customer data, including Social Security numbers. Learn more about the chaotic events, the cunning hackers behind them, and what it means for cybersecurity in today's interconnected world.

Read the Story →

How to Prevent eCommerce Phishing

Educate your team and customers

Regularly update your team and customers about the latest phishing schemes and social engineering techniques. Teach your team how to scrutinize emails, links, and attachments to ensure they are safe. Perform simulated phishing attacks to train employees to recognize and respond appropriately to phishing attempts.

Implement advanced security measures

Utilize email filtering, web filtering, and anti-phishing software to detect and block phishing attempts.

Secure your website

Ensure your website uses HTTPS and educate customers to look for the security padlock in their browser before entering any personal information.

Add an extra layer of security to ALL accounts

Require all customers to set up multi-factor authentication (MFA) for store accounts; require the same of employees for all the tools they use for work.

Regularly monitor and audit your systems

Regular checks can help detect any unusual activity and prevent potential breaches.

RELATED THREAT

Man-in-the-middle (MitM) attacks

Eavesdropping on or altering the communication between two parties to steal or manipulate data. For example, a cyber attacker sets up a rogue Wi-Fi hotspot with a name similar to a legitimate one, such as in a coffee shop. Once a customer connects to the rogue Wi-Fi network, the attacker can monitor and intercept all the data transmitted between the customer's device and an eCommerce site. As the customer submits their payment details (credit card number, expiration date, CVV), the attacker captures this information in real-time through the compromised network connection.

A RECENT CASE OF MITM

Man-In-The-Middle Flaw Left Smartphone Banking Apps Vulnerable

Read the Story →

First-Party Fraud: The Ultimate Customer Betrayal

First-party fraud is particularly insidious and challenging to detect among all the types of eCommerce fraud. It's possible that even our favorite customers may have engaged in this type of fraud at some point, as 35% of shoppers have admitted to committing first-party fraud, with 34% citing economic hardship as their reason for doing so. Financial challenges are making it easier for good citizens to justify fraudulent behavior. Unfortunately, it's still fraud and has a negative impact on revenue for businesses. Unlike traditional fraud that involves identity theft, first-party fraud is committed by consumers using their own identity, or a synthetic one they've created, to make purchases or obtain credit with no intention of repayment.

What is First-Party Fraud?

First-party fraud occurs when a legitimate online shopper deliberately engages in fraudulent activities to gain a financial advantage or obtain goods or services without intending to pay for them. This form of fraud is committed directly by the consumer, without the involvement of an external fraudster or identity thief. Unlike traditional fraud schemes that often involve stolen credit card information or account takeover, first-party fraud involves deceitful actions by the account holders themselves.

How First-Party Fraud Happens

Friendly fraud or chargeback fraud

When a consumer makes a legitimate transaction and then disputes it as fraud or unauthorized to avoid payment.

Return fraud or refund abuse

Customers exploit a merchant's return policy by claiming a product was not as described, faulty, or that an item was not received (INR) to secure a refund or replacement while retaining the original item.

Overstating financial information

Individuals inflate their income or assets on credit or buy now pay later (BNPL) applications to qualify for purchases they have no intention of repaying.

How to Prevent First-Party Fraud

Monitor shopper behavior and block repeat offenders

Use advanced analytics to detect unusual shopping patterns like high return rates. Set alerts so your fraud analysts or customer service representatives can further investigate suspicious accounts. Add repeat offenders to your fraud prevention solution's blocklist so future transactions are automatically rejected.

Report repeat offenders to their financial institution

Maintain an effective chargeback management process by keeping thorough records of all transaction details. Report repeat offenders to their bank or credit card company so they can take further action — and provide all the evidence you've compiled over multiple transactions.

Create dynamic return policies

Tailor return policies based on customer history and risk profiles to prevent exploitation. For riskier customers, establish stricter refund policies, such as shorter return windows or requirements for original packaging and receipts, to deter fraudulent returns.

Regularly audit returns and chargebacks

Conduct regular audits of returned items to ensure they match the product descriptions and conditions as claimed by the customers. Audit chargeback transactions and look for patterns that may be indicative of fraud.

Follow chargeback prevention best practices

Before a customer makes a purchase, the best approach a business can take is to make sure they're delivering a premium pre-purchase experience. Are your product descriptions clear and accurate? Is the return policy clearly posted and easy to understand? And after purchase, make sure to continue the experience by delivering white-glove-level customer service. A great customer experience can be a strong deterrent for friendly fraudsters, who may feel guilty scamming a brand they've grown to love.

A FIRST-PARTY FRAUD STORY WITH A HAPPY ENDING

G8Only Conquered a Rising First-Party Fraud Trend Using NoFraud

G8Only noticed a rise in chargebacks from repeat customers, as well as consumers whose credit card information was stolen. The increase in chargebacks was leaving them with massive fraud fees from their payment processor, lost revenue and merchandise, and hundreds of hours each month spent fighting chargebacks. The team was unhappy with its fraud prevention solution because it wasn't performing as needed.

As the business continued to grow, so did fraud. G8Only founder, Joe LaBruzza noticed, **"It's a numbers game. Say 5% of your transactions are fraudulent; 5% of $100,000 doesn't sound like much, but 5% of $1 million? …It just gets worse."**

Determined to keep more of their hard-earned revenue, the G8Only team started to analyze their data for fraud patterns. They were able to identify ways to prevent fraud by modifying processes and regions they sold to, but it ultimately blocked growth. They needed a way to seamlessly automate fraud prevention so it didn't add friction to the customer experience while minimizing revenue loss.

Read about G8Only's full fraud-fighting journey →

Stolen Identities: Unauthorized Purchases

> Unauthorized purchases are the underlying threat to eCommerce when it comes to the alarming trends we're seeing across identity theft, card testing, and account takeover (ATO) attacks. These varying angles of stolen identities are creating a complex web of threats for businesses and consumers alike. Over the last five years, there has been a 68% increase in identity theft cases. Parallel to this, there has also been a spike in card testing, with as many as 85% of merchants saying they've experienced this type of fraud. Card testing causes direct financial losses and also serves as a gateway to broader payment fraud, allowing criminals to authenticate stolen credit card information for larger, more damaging purchases.

Fraudulent purchases make up 34% of all chargebacks. The cumulative effect of identity theft, card testing, and ATO attacks on chargebacks exacerbates operational challenges, elevating dispute resolution costs and potentially increasing penalty fees from credit card companies, making it a multifaceted problem that affects the entire payment ecosystem.

What is Identity Theft?

Identity theft involves the unauthorized acquisition and use of someone's personal information — such as their name, social security number, or credit card details — to commit fraud or theft. In the context of eCommerce, this can lead to unauthorized transactions, account takeovers, and the opening of fraudulent accounts, causing significant financial and reputational damage to both consumers and businesses.

What is Card Testing?

Card testing, also known as carding, is a subset of identity theft in which criminals test stolen credit card numbers to verify their validity and credit limit. Fraudsters will use small transactions on websites, online services, or donation platforms that have automated payment processing systems to confirm if the stolen card details can be used for larger fraudulent purchases.

What is Account Takeover?

Account Takeover occurs when an unauthorized party gains access to a shopper's eCommerce account, enabling them to make unauthorized purchases, siphon funds, or pilfer sensitive personal data. This fraud not only results in financial losses but can also severely damage customer trust and brand reputation.

How Stolen Identities & Unauthorized Purchases Happen

Phishing attacks

Cybercriminals acquire credit card details or account passwords through phishing, data breaches, or purchasing them on the dark web. Fraudsters may deceive shoppers — using manipulative social engineering tactics — into revealing their login credentials through fake emails or websites masquerading as legitimate businesses. Merchants can also become victims of social engineering as fraudsters trick eCommerce teams into granting access to a customer's account.

Data breaches

Cybercriminals hack into databases of eCommerce sites to steal the personal and financial information of customers.

Credential stuffing and automated testing

Cybercriminals hack into databases of eCommerce sites to steal the personal and financial information of customers.

Validation and exploitation

Once a card or account is verified as active, it's used for larger fraudulent purchases or sold to other criminals.

Chargebacks and losses

Merchants face chargebacks from legitimate cardholders, incurring fees, losing out on merchandise, and consequences from exceeding chargeback thresholds.

How to Prevent Unauthorized Purchases

Monitor transactions and perform velocity checks

Implement systems to detect unusual transaction patterns, such as multiple attempts with different cards from the same IP address or logins from new devices or locations, which could indicate an ATO attempt. Use advanced fraud detection solutions that use real-time machine learning to identify and block suspicious activities.

Integrate CAPTCHA verification on payment gateways

The CAPTCHA mechanism can deter automated bots from testing card details on your site.

Employ multiple lines of authentication

Card verification value (CVV) and address verification services (AVS) can help verify that the customer possesses the physical card. Consider using MFA or 2FA for all transactions or those that are flagged as high-risk to ensure the cardholder is authorizing the purchases.

Data encryption

Utilize robust encryption standards for storing and transmitting customer data to protect it from unauthorized access.

Keep up with the latest compliance standards

Adhere to data protection regulations like GDPR and PCI DSS to ensure the highest standards of data security and privacy.

Monitor for exposed information

Use services that monitor the dark web for leaked or stolen data, allowing for prompt action if customer information is compromised.

Impart account security best practices on customers

Educate customers about the risks of phishing and the importance of secure password practices, including not reusing passwords across sites. Encourage shoppers to install reputable antivirus and anti-malware solutions on their devices to prevent keylogging and spyware.

Stay apprised of where you stand in relation to chargeback thresholds

Chargeback thresholds are predefined limits set by payment processors or acquiring banks that determine when a merchant may face consequences due to excessive chargebacks. These thresholds are in place to monitor and manage the level of chargebacks a merchant experiences, as high chargeback rates can have negative consequences for both the merchant and the payment processor.

Create effective password policies to protect accounts

Encourage or enforce strong, unique passwords through regular prompts and by blocking common or previously breached passwords. Implement stringent verification processes for any account change requests, especially those made via customer service channels.

Perform frequent security audits

Conduct periodic reviews of account security measures, and update them in response to new or evolving threats.

PRO TIP

Irina Vayner,
Sr. Fraud Analyst at NoFraud

"It's always interesting to see the different ways fraudsters will try to manipulate information to make orders appear legitimate. Merchants should be wary of shoppers who make repeated calls attempting to confirm an order's legitimacy. Their demeanor can be convincing over the phone, but fraudsters are adept at social engineering, often saying exactly what is needed to win over the trust of customer service representatives, masking the illegitimacy of their orders."

Related Threats

Payments fraud

Card testing falls into the realm of payments fraud, which includes any fraudulent or unauthorized activity that occurs during a payment transaction, typically involving the use of stolen payment information or deceptive practices to gain financial benefit illegally.

Credit grooming or bust-out fraud

A scheme where fraudsters build good credit over time using stolen or synthetic identities only to max out their credit limits without any plans of repayment.

Synthetic identities

Combining real and fake information to create new identities used to open fraudulent accounts or make purchases.

Promo & Policy Abuse: Exploiting eCommerce Generosity

Discounts, coupons, refund policies, and loyalty programs are all part of creating an optimal shopping experience for good customers with a goal of driving more engagement. Unfortunately, the increasing prevalence of scammers abusing these programs has become a significant concern. Promo abuse costs U.S. businesses up to $600 million per year with 73% of merchants reporting that they've experienced this type of fraud. As online shopping continues to surge, so does the opportunity for abuse, challenging merchants to find a balance between offering promotions to attract genuine customers and protecting their bottom line.

What is Discount/Coupon Abuse?

Discount and coupon abuse occurs when individuals or groups exploit promotional offers, using them in ways not intended by the retailer, such as using a single-use code multiple times.

What is Refund Abuse?

Refund abuse involves manipulating return policies to receive refunds for items that are not eligible for return, have been used, or in some cases, not returned at all.

How Promo & Policy Abuse Happens

Multiple redemptions

Shoppers use technical loopholes or create multiple accounts to redeem single-use coupons multiple times.

Promo code sharing

Exclusive or personalized promo codes are shared on deal sites, leading to widespread unauthorized use.

Exploiting return policies

Buyers purchase items with the intention of using them temporarily, then return them for a full refund, a practice known as "wardrobing" or "free renting."

Friendly fraud for refunds

Customers claim an item was never received or falsely report it as damaged or not as described to secure a refund while retaining the product.

How to Prevent Promo & Policy Abuse

Keep coupon codes secure

Implement secure, single-use coupon codes and monitor for unusual redemption patterns.

Offer personalized promotions

Tailor discounts and coupons to individual customers and require account login for redemption to prevent sharing.

Purchase limitations

Set purchase limits for high-demand or discounted items to deter bulk buying and resale.

Refund verification

Require proof of purchase and inspect returned items carefully before processing refunds. Consider offering store credit instead of cash refunds for certain cases.

Make return policies clear

Define and communicate clear return policies, including conditions for refunds, restocking fees, and time limits. Clearly communicate the terms and conditions of promotions and the consequences of abuse to foster a culture of honesty and integrity among customers.

Keep up to date with the latest trends in refund and return fraud

New forms of refund abuse are constantly popping up as fraudsters navigate loopholes to exploit. Stay ahead of their tactics and ensure your fraud prevention solution is leveraging machine learning to block bad actors from completing transactions.

RELATED THREAT

Reseller fraud

Reseller fraud, also known as reseller abuse, is the unauthorized sale of products or services through online marketplaces. Reseller fraud happens when a reseller distributes a product without having an official relationship or agreement with the original merchant. Fraudulent resellers will oftentimes take advantage of promotional pricing to score high volumes of discounted merchandise to turnaround at a higher price point. Such resellers often do not adhere to the original brand's pricing, warranty, or service standards, leading to issues with product quality and customer satisfaction.

A RETURN FRAUD STORY WITH A HAPPY ENDING

Raycon Conquered a Rising Return Fraud Trend Using NoFraud

Raycon noticed an uptick in fraudsters placing orders for thousands of dollars worth of new products with the intention of returning empty boxes — likely a scheme to commit reseller fraud. Thanks to his strategic partnership with NoFraud, the team was notified of the rising return fraud trend a week prior, so they knew just what to look for.

"We were doing whack-a-mole as these orders were coming in," Jim Schreiber, Vice President of Operations at Raycon, said of the experience. The amount of fraud was racking up at a startling pace and the return fraud attack was costing the company thousands of dollars per hour. Before this crazy day was over, Jim was able to work with the NoFraud team, working with programmers to set up effective fraud defenses and ensure their backend infrastructure was secure. They ended up blocking $200,000 in fraud that day.

Read about Raycon's full fraud-fighting journey →

Loyalty Fraud: Undermining Customer Trust in eCommerce

> Loyalty fraud has seen a significant uptick in incidents, with one in five businesses reporting millions of dollars in annual losses. This type of fraud directly targets customer loyalty programs, exploiting them for unauthorized gains and, in the process, eroding the trust and value these programs are designed to foster between businesses and their customers.

What is Loyalty Fraud?

Loyalty fraud occurs when individuals exploit loyalty programs by illegitimately earning or redeeming points or rewards. This can be achieved through account takeover, creating fake accounts, manipulating program rules, or using stolen credit card information to accrue points. Such activities not only lead to financial losses but also damage the integrity of loyalty programs, affecting genuine customers and the brand's reputation.

How Loyalty Fraud Happens

Account takeover

Fraudsters will launch an account takeover attack to gain unauthorized access to customers' loyalty accounts to redeem points for products, gift cards, or other rewards.

Point generation schemes

Exploiting loopholes in the loyalty program to generate points illegitimately, such as through fake purchases or referral fraud.

Synthetic account creation

Using false identities to create multiple accounts and accumulate rewards, often automating activities to meet point-earning criteria.

Reward trafficking

Selling or trading loyalty points or rewards on unauthorized third-party platforms.

How to Prevent Loyalty Fraud

Always use secure authentication methods

Implement multi-factor authentication (MFA) for accessing loyalty accounts, adding a layer of security against unauthorized access. Enforce strict verification processes for high-value redemptions or changes to account details to prevent unauthorized transactions.

Monitor transaction patterns

Use a fraud prevention solution that offers advanced analytics to identify unusual redemption patterns or point accruals that may indicate fraudulent activity.

Limit reward transferability

Restrict the ability to transfer points or rewards between accounts or limit the sale/trade of rewards on external platforms.

Regularly update program terms

Review and update loyalty program rules to close loopholes that could be exploited for fraud.

Affiliate Fraud: Eroding the Foundations of Partnership Marketing

Affiliate marketing, a cornerstone strategy for driving sales and enhancing brand visibility in eCommerce, is increasingly compromised by affiliate fraud. Merchants around the world reported $3.4 billion in losses with 22% experiencing affiliate fraud. This fraudulent activity jeopardizes the trust between merchants, affiliate networks, and genuine affiliates. Understanding and mitigating affiliate fraud is imperative to maintain the integrity and effectiveness of affiliate marketing programs.

What is Affiliate Fraud?

Affiliate fraud involves manipulating affiliate marketing systems to earn commissions or rewards dishonestly. This can include generating fake leads or sales, using stolen credit card information to complete purchases, or artificially inflating traffic statistics. Such deceptive practices undermine the fairness and profitability of affiliate marketing programs.

How Affiliate Fraud Happens

Fake leads or transactions

Fraudsters generate bogus leads or sales using automated scripts or stolen user information to claim undeserved commissions.

Click fraud

Click fraud artificially inflates click counts through automated bots or hired individuals to increase commission earnings without genuine customer engagement.

Cookie stuffing

Cookie stuffing secretly drops affiliate cookies on users' computers without their knowledge, falsely claiming credit for user purchases.

Typosquatting

Typosquatting registers misspelled versions of popular domain names to redirect users through affiliate links without their explicit intent to visit the merchant's site.

How to Prevent Affiliate Fraud

Be vigilant in vetting affiliates

Thoroughly screen and monitor affiliates before and after approval to ensure they adhere to ethical practices. Continue to monitor them during your partnership, auditing affiliate activities and verifying the legitimacy of transactions and the methods used to generate traffic.

Use advanced fraud detection tools that can protect against affiliate fraud

Employ sophisticated detection technologies that analyze patterns in real-time that are indicative of affiliate fraud, such as abnormal conversion rates or suspicious IP addresses.

Provide clear program guidelines to affiliates

Establish and communicate clear rules and guidelines for affiliate conduct, explicitly prohibiting fraudulent practices and outlining the consequences. Define what acceptable marketing practices look like and the importance of maintaining the program's integrity for mutual benefit.

Reshipping Scams: Organized Fraud Rings Exploiting Good People

The eCommerce landscape faces a pervasive threat from reshipping schemes, contributing to global fraud losses that extend into billions of dollars. These schemes facilitate the movement of illicit goods while placing unsuspecting individuals at risk of criminal involvement. The Better Business Bureau Scam Tracker reported that 65% of scam job offers were tied to involve reshipping. The growing sophistication of organized crime networks emphasizes the need for heightened awareness and prevention strategies.

What is Reshipping?

Reshipping schemes involve the use of individuals to move stolen goods. Individuals (often unknowingly) are recruited to receive and then forward packages containing merchandise purchased with stolen credit card information.

How Reshipping Scams Happen

Recruitment

Fraudsters recruit individuals through job postings, social media, or email campaigns, offering work-at-home opportunities that involve receiving and reshipping packages.

Stolen credit information

Cybercriminals use stolen credit card details to purchase high-value items online, which are then shipped to the addresses of recruited reshippers.

Reshipping

The recruited individuals forward the packages, often to addresses abroad, effectively obscuring the trail of stolen goods.

How to Prevent a Reshipping Scam

Only sell to verified customers

Implement stringent verification processes for new accounts or high-value transactions to detect potential fraudulent activity.

Monitor shipping and transactions

Utilize advanced monitoring systems to identify suspicious patterns, such as multiple shipments to addresses linked to known fraud or unusual transaction volumes.

Launch awareness campaigns

Educate the public about the risks and indicators of being recruited as a reshipper, highlighting the legal consequences.

Collaborate with law enforcement

Work closely with postal services and law enforcement agencies to report and investigate suspicious activities.

Create secure payment processes

Strengthen payment processing systems to detect and prevent the use of stolen credit card information.

Botnets: The Silent Army Behind eCommerce Fraud

Botnets are used to infect computers with malware and conduct fraudulent activities, undermining the security and integrity of online businesses. The automation and scale at which botnets operate make them a formidable threat, capable of evading detection and bypassing traditional security measures. A study found that 57% of eCommerce website attacks are carried out through the use of botnets. And within the last year alone, there has been a 16% increase in botnet command and control servers.

What are Botnets?

Botnets refer to networks of hijacked computers and devices that are controlled by cybercriminals to execute automated tasks targeting online retail platforms and their users. These botnets are utilized for various malicious activities, including launching distributed denial-of-service (DDoS) attacks to disrupt website operations, executing credential stuffing attacks to gain unauthorized access to user accounts, and conducting fraudulent transactions. The automation and scale of botnets allow attackers to perform these activities at a high volume and speed, posing significant security challenges for eCommerce sites in protecting their infrastructure and safeguarding customer information against theft and abuse.

How Botnets Operate

DDoS attacks

Botnets overwhelm eCommerce websites with traffic from multiple sources, rendering the site inaccessible to legitimate users (customers and shop employees) and can cause significant downtime and revenue loss.

Credential stuffing and card testing

Botnets are used to automate login attempts using stolen username and password combinations across multiple websites to gain unauthorized access to user accounts. Similarly, bots are used to test stolen credit card information on eCommerce platforms, identifying valid card details for larger fraudulent purchases.

Phishing

Bots are also used to conduct large-scale phishing attempts or spam to steal personal information or spread malware.

Scraping

Botnets can scrape pricing, product descriptions, or other proprietary data from eCommerce sites to gain a competitive advantage or create counterfeit listings for a fake storefront.

How to Prevent Botnet Schemes

Use advanced traffic filtering tools

Deploy solutions that can distinguish between legitimate users and bot traffic, blocking malicious bots while allowing genuine customers access.

Implement CAPTCHA verification

CAPTCHAs are designed to challenge suspicious login attempts or checkout activities, making it harder for bots to proceed.

Implement access limits

Set limits on the number of requests an IP address can make in a certain timeframe to prevent automated attacks.

Perform frequent system audits

Conduct security audits and vulnerability assessments to identify and patch potential entry points for malware.

Collaboration with ISPs and authorities

Work with internet service providers and law enforcement to report and take down botnet command and control servers.

PRO TIP

Ibtissam El Ansari,
Sr. Fraud Analyst at NoFraud

"As cyber threats continue to evolve, the implementation of 2FA or MFA remains a key defense mechanism for online businesses aiming to protect their assets and customers. Be sure customer accounts and business accounts have MFA enabled. This added layer of security makes it difficult for bots to bypass."

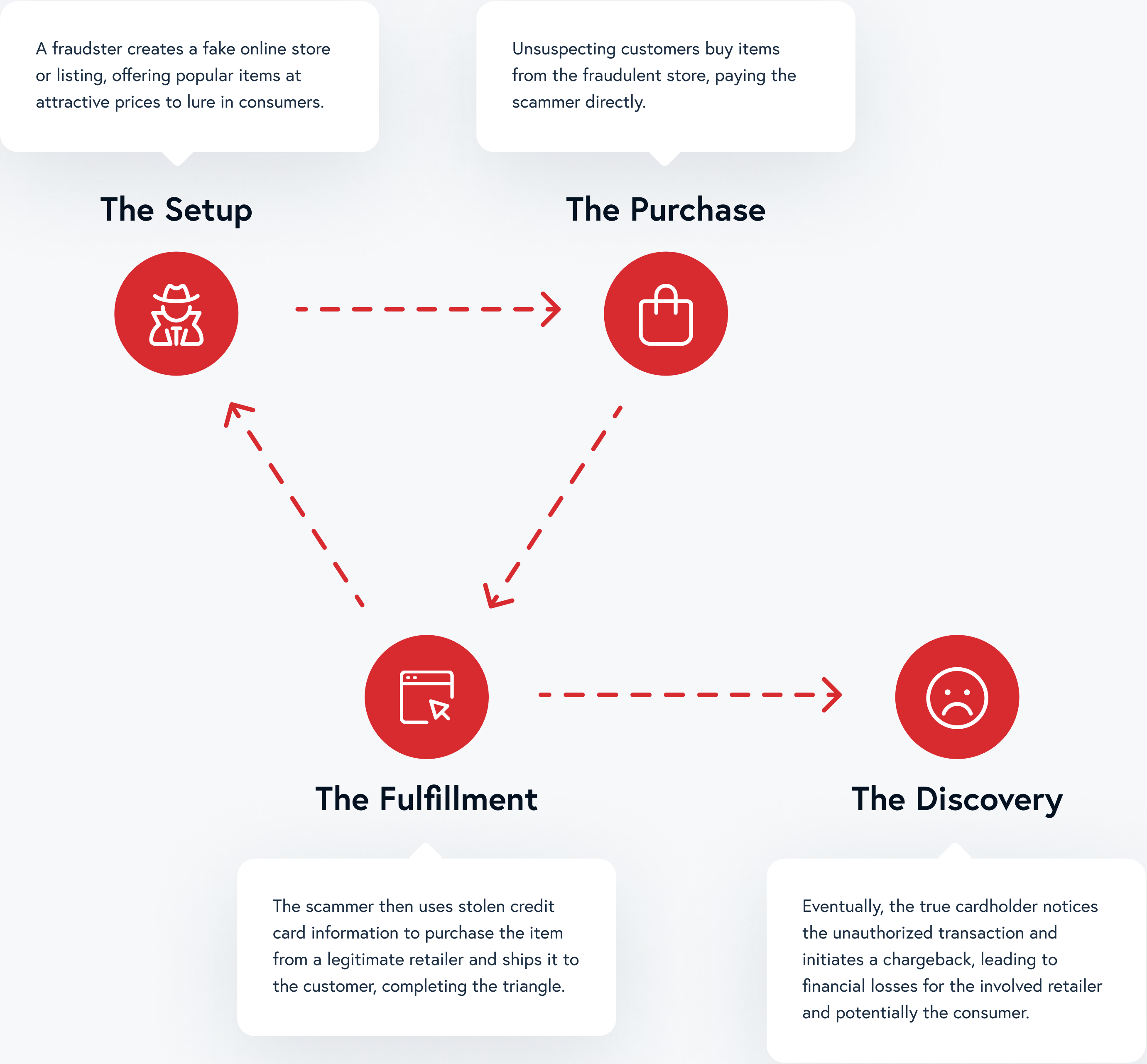
Triangulation Fraud: The Deceptive Triangle in eCommerce

Triangulation fraud has emerged as a sophisticated scam that has increased by 70% within the past year. This type of fraud involves three entities: the unsuspecting consumer, the fraudulent seller, and the legitimate online marketplace. Customers think they're getting an authentic brand experience, but in reality, they're shopping at a fake storefront with scammers hiding behind it. Triangulation fraud schemes cause substantial financial losses for eCommerce shops and erode customer trust, leaving many victims unaware they've been scammed until it's too late.

What is Triangulation Fraud?

Triangulation fraud occurs when a fraudster sets up a fake storefront on an eCommerce platform or a standalone website, offering high-demand goods at significantly lower prices. When consumers purchase these items, the fraudster uses stolen credit card information to buy the goods from another retailer and ships them to the consumer, pocketing the difference. The consumer receives the item, but the transaction is fraudulent, leaving the cardholder to dispute unauthorized charges.

How Triangulation Fraud Happens



The Setup

A fraudster creates a fake online store or listing, offering popular items at attractive prices to lure in consumers.

The Purchase

Unsuspecting customers buy items from the fraudulent store, paying the scammer directly.

The Fulfillment

The scammer then uses stolen credit card information to purchase the item from a legitimate retailer and ships it to the customer, completing the triangle.

The Discovery

Eventually, the true cardholder notices the unauthorized transaction and initiates a chargeback, leading to financial losses for the involved retailer and potentially the consumer.

How to Prevent Triangulation Fraud

Enhance seller verification methods

Marketplaces should implement strict seller verification processes to prevent fraudsters from setting up shop.

Let shoppers know about fake stores

Educate consumers on the risks of triangulation fraud and encourage them to report suspiciously low prices or sellers.

Monitor the web for copycat websites

Use Google Alerts or a similar tool that can flag duplicate websites or product listings so you can vet whether or not they're authorized sellers. Take action to get fraudulent sites shut down by reporting them to authorities.

Secure and monitor transactions

Use secure, encrypted payment gateways that verify the authenticity of transactions and protect consumer data to ensure stolen credit cards aren't being used. Implement advanced fraud detection systems that flag unusual purchasing patterns indicative of stolen card use. Employ additional verification steps for transactions that present a high risk of fraud, such as cross-referencing shipping and billing addresses.

TRUE CLASSIC

A TRIANGULATION FRAUD SCHEME WITH A HAPPY ENDING

True Classic Conquered Triangulation Fraud Using NoFraud

True Classic was surprised when they were hit with a return fraud spike. In working with NoFraud, they learned fraudsters had been scheming — on the dark web — to take advantage of the company's return policy. The scheme was tied to fake storefronts popping up online, a triangulation fraud scheme that threatened their brand, customers, and revenue.

NoFraud was able to set up effective detection mechanisms to stop further damage from return policy abusers, while ensuring their business continued to run smoothly.

"I didn't realize how proactive we could be in stopping fraud and minimizing risk. There is a whole business method that goes into preventing fraud," Breanna Moreno, VP of CX at True Classic, shares.

Read about True Classic's full fraud-fighting journey →

NOFRAUD

About NoFraud

Founded in 2014, NoFraud is an eCommerce checkout and fraud prevention pioneer, ensuring every eCommerce merchant has access to the services and protection they need to scale with confidence. The company provides online merchants with cost effective, easy-to-use solutions that remove friction and fraud from their eCommerce funnel to grow sales and improve the purchase experience for customers.

NoFraud provides the industry's most accurate eCommerce fraud protection solutions to increase merchants' conversion and approval rates while virtually eliminating fraud. Visit www.nofraud.com for more information.

Ready to learn more?

Book a demo to see how NoFraud improves your bottom line by approving more orders and relieving the burden of manual review.

Book Demo →

Get in touch with a Fraud Expert. 888-773-3669 sales@nofraud.com nofraud.com