BrandShield® | SOFTPROM

The Dark Side of Holiday Shopping

Why Brands Need Protection Against Counterfeiters

—

Nov 2024 | BrandShield Data Center

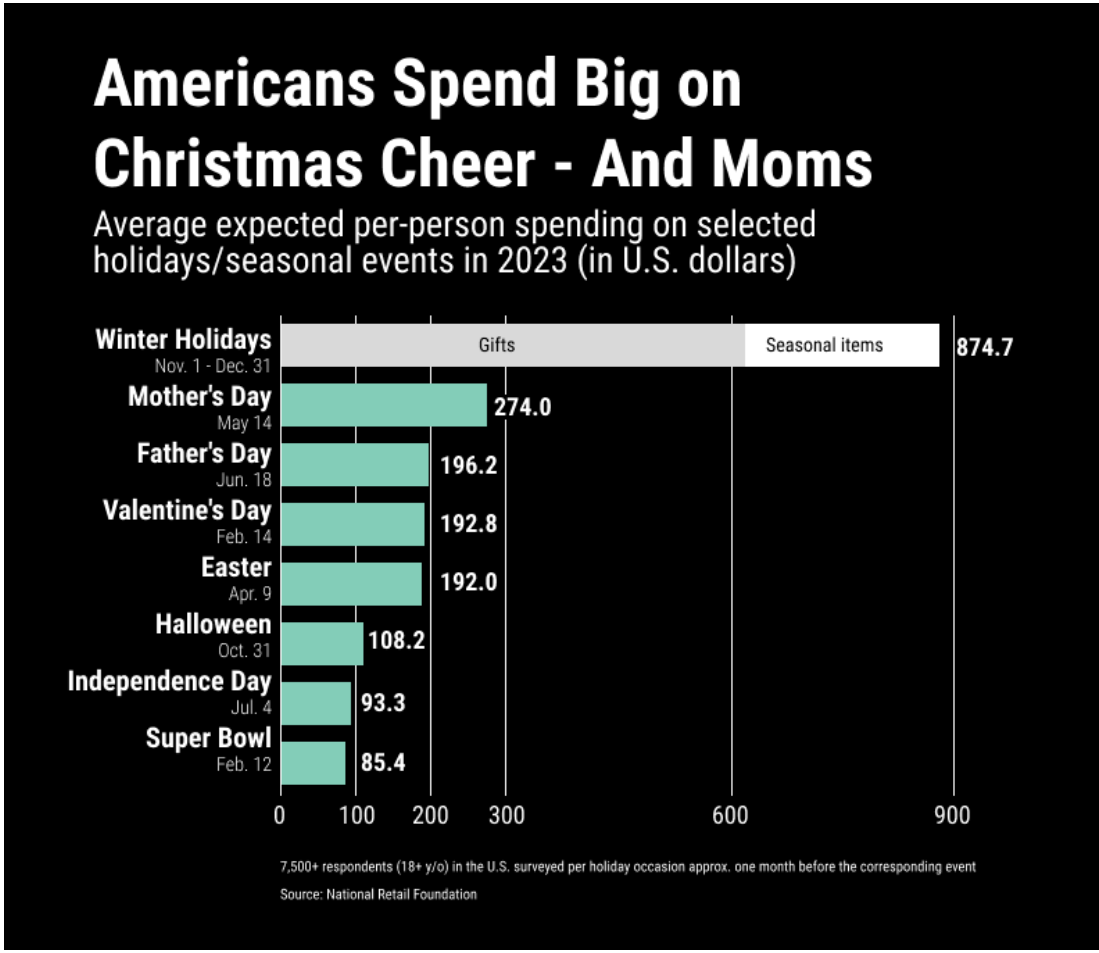
BrandShield®

'Tis the Season to Protect Your Brand

As sleigh bells ring and the excitement of holiday bargains approaches, both shoppers and counterfeiters are gearing up for some serious shopping action. While eagerly anticipating lighning deals on special gifts, consumers and brand owners alike need to be aware that a dark, sinister threat is lurking under the surface, waiting and watching. With more people than ever shopping online, the threat of savvy fraudsters is growing, and with their increase in sophisticated techniques, the season of giving is quickly becoming an opportunity for taking.

Since Covid-19 online shopping has increased year on year at an unprecedented rate, a trend that's only intensified with the number of people shopping online. The "holiday shopping season" has evolved far beyond its traditional November and December months with Black Friday, Cyber Monday and Christmas, with retailers such as Amazon and Walmart starting to entice customers as early as October with discounts and offers that can't be refused. This extended shopping season has only created more opportunities for fraudsters who mimic brand websites, sell counterfeit goods, and prey on unsuspecting consumers. Brands now face a critical challenge that can't be ignored any longer. Each successful scam not only results in financial losses but also eroding the trust that brands have worked so hard to build.

This eBook discusses the various scams that emerge during the holiday rush, where they can be detected, and the proactive steps brands can take to protect both their customers and their pockets.



BrandShield

Everyone Loves a Good Bargain, But What Could Go Wrong?

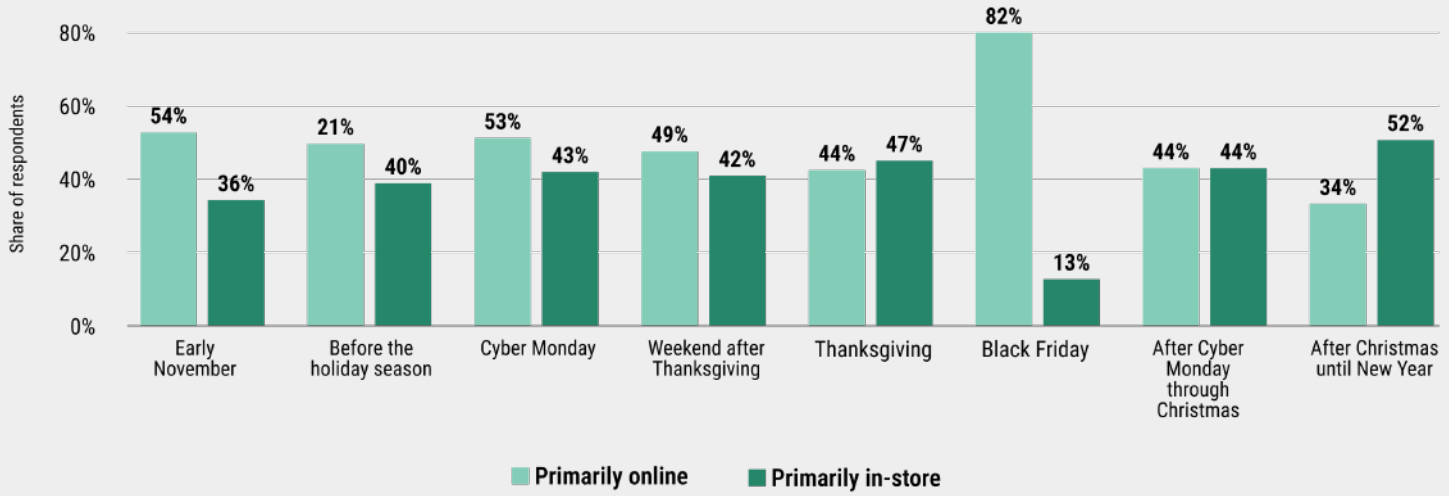
The explosive growth in e-commerce continues to shatter records, with global online retail sales projected to reach $8.1 trillion by 2026. The 2023 holiday season alone saw U.S. consumers spend $222.1 billion online, marking a 4.9% increase from the previous year.

This massive volume of transactions is precisely what makes the holiday season particularly vulnerable for brand owners. During peak shopping days like Black Friday, the sheer number of transactions makes monitoring and detecting fraudulent activity exponentially more challenging. Counterfeiters exploit the hype around these shopping daysby setting up lookalike websites, advertising fake goods and using fake ads on social media. Unsuspecting customers often end up not receiving their items, and often lose money in the process.

In addition, the hybrid shopping model that emerged post-pandemic, combining online convenience with occasional in-store visits, has created new opportunities for scammers. Social media scams alone caused $2.7 billion in consumer losses in 2023, with holiday-themed fraud seeing a particularly sharp increase. Brand owners must now pay attention to an ever-expanding digital landscape, from marketplace listings to social media impersonations.

Online vs. in-store shopping for the holiday season in the United States in 2024

Statista, 2024



BrandShield®

What Brands Gain in Sales, Can Be Lost in Scams

According to CBS News, $2 trillion worth of counterfeit products are sold each year. The imitation products are becoming increasingly hard to identify and in some cases can be harmful. The counterfeit goods are often made with substandard materials and tend to have short life spans. The story of counterfeits is not new, but the sophistication of scammers is becoming harder to deal with. Fashion Brands like Gucci, Prada, Michael Kors, Adidas, Nike, and Levi's are some of the worst affected.

But, the true cost of counterfeiting to brands extends far beyond lost revenue. While many consumers do have a negative opinion towards counterfeit products, a significant portion believe the fault lies with the brand itself for not doing enough to protect them from the threat. According to a survey by Potter Clarkson, 34% of the consumers surveyed said they wouldn't even buy from a brand's own website if the brand had been susceptible to counterfeits elsewhere online in the past. It is undeniable that brand reputation can be seriously damaged and further harm customer trust and loyalty.

Not only that, but the fallout from these counterfeit purchases puts immense pressure on customer service teams, who are left to handle frustrated consumers, process refunds, and spend valuable time educating buyers on spotting unauthorized sellers. This relentless drain of resources and reputation damage can cause a severe risk to the brand's long-term success and its hard-earned relationship with its customer base.

$2T worth of counterfeit products are sold each year.

CBS News

34%

of the consumers surveyed said they wouldn't even buy from a brand's own website if the brand had been susceptible to counterfeits elsewhere online in the past.

www.potterclarkson.com/insights/how-does-counterfeiting-affect-brands/

BrandShield®

The How, Why and Where Scams are Taking Place

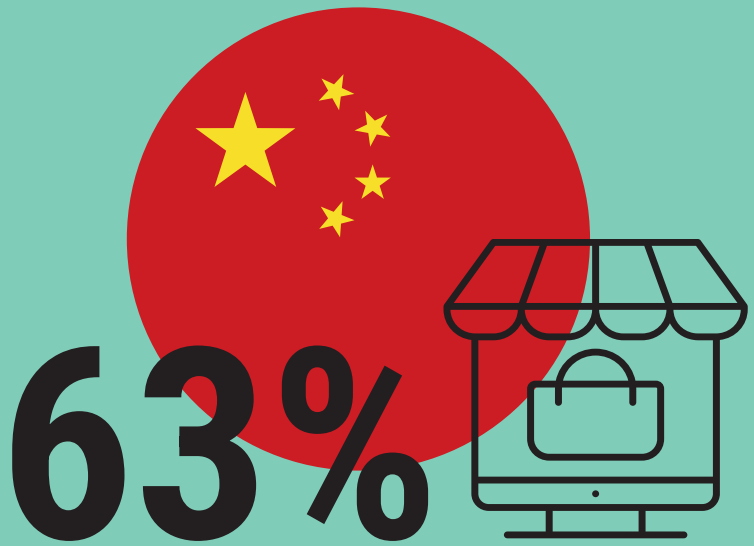
Counterfeit Sales

Counterfeiters create convincing replicas of popular brands, quickly capitalizing on well-known logos, designs, and packaging. By mimicking established brand products, they exploit consumer trust, making people think they're purchasing the real thing at a much better price. With sophisticated counterfeits or "superfakes," even experienced shoppers have been known to struggle with what is real from what is fake. With over $2 trillion worth of counterfeit products being sold each year, it's quite easy for a brand's reputation to be tarnished and cause great customer dissatisfaction.

Phishing Scams and Fake Websites

Phishing scams skyrocket during high-traffic shopping times like the holiday season. Fraudsters design look-alike websites or emails with minor changes in URL (like an extra letter or number) to trick consumers into believing they're on the official site. These fake sites can request login details, payment information, and other sensitive data, which can lead to identity theft and financial loss for unsuspecting consumers. Phishing scams, according to the Anti-Phishing Working Group, have doubled in recent years, making this a key threat that brands need to monitor closely, especially during peak shopping seasons.

RETAILERS MUST PAY ATTENTION



63%

of Western consumers plan to purchase from Chinese shopping applications

Gray Market

The gray market involves selling genuine branded products through unauthorized channels. Though the items themselves aren't counterfeit, they're distributed outside of the brand's approved retail networks, often at a reduced price, which undercuts the brands revenue stream considerably. This naturally can lead to warranty issues, lower-quality customer service, and can harm brand exclusivity, eroding trust. Brands like luxury retailers or electronics manufacturers are particularly vulnerable to gray market activities, which can compromise customer experience and erode pricing control. In many cases, although the gray market is not illegal on its own, you can still remove gray market sites, social pages and marketplace listings. In order to do that however, you need a deep understanding of ecommerce and the online markets and have the expertise and knowledge regarding IP laws.

Trademark Infringement

Fraudsters have mastered the art of brand deception, weaponizing trusted trademarks, logos, and slogans to orchestrate elaborate schemes across digital platforms. These sophisticated criminals skillfully craft fake social media profiles and marketplace listings that are increasingly difficult to distinguish from legitimate brand presence. Their strategy is mostly simple yet ultimately devastating. The impact for brands extends far beyond lost sales. When customers receive counterfeit products or fall victim to scams, their negative experiences are automatically associated with the legitimate brand, creating lasting damage to brand reputation and consumer trust. These trademark violations are particularly rampant on major social media platforms like Instagram, Facebook, and Twitter, as well as leading e-commerce marketplaces such as Amazon and eBay. During the holiday season, in particular, this problem intensifies as fraudsters capitalize on the increased consumer spending and the chaos of time-sensitive deals to push their counterfeit operations into overdrive.

BrandShield®

How to Keep Your Brand Functioning and Free of Scams

Implement Advanced Monitoring

In today's online marketplace, brands need a robust digital monitoring system that includes AI-powered scanning tools to identify counterfeit listings across multiple platforms. Continuous, 24/7 monitoring of social media and marketplaces enables brands to catch unauthorized listings, fake profiles, and malicious activity as it arises. With new platforms and trends constantly emerging, staying ahead of threats requires both vigilance and adaptable monitoring solutions to protect brand reputation.

Take Immediate Action

Once a threat is detected, immediate action is crucial to minimize the damage. Brands can benefit from automated takedown procedures that expedite the removal of counterfeit listings and infringing profiles. Real-time notification systems alert enforcement teams to any suspicious activity, allowing them to respond quickly and effectively. Coordinated legal responses can also help enforce a brand's rights across jurisdictions, ensuring counterfeiters face the consequences and deterring future violations.

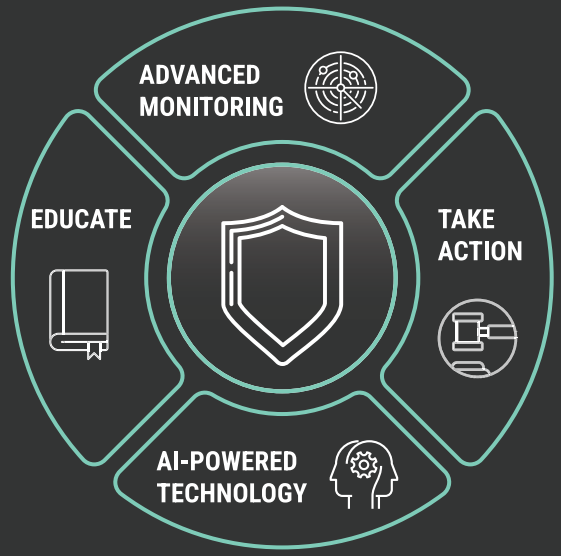
Educate Your Customers

An informed customer base is a powerful defense against counterfeiters. Providing clear authentication guides helps buyers recognize legitimate products, while verified seller lists give them reliable options for making purchases. Offering direct reporting channels encourages customers to alert brands of suspicious listings, creating a partnership in protection.

Utilize AI-Powered Technology

Incorporating advanced technologies is key to enhancing brand protection efforts. Blockchain authentication, for example, provides a secure, traceable way to verify genuine products, making it difficult for counterfeiters to replicate authenticity. AI-powered threat detection can analyze patterns in real-time, flagging suspicious activities before they escalate. Digital watermarking embeds unique, traceable identifiers into products or images, adding another layer of protection that strengthens a brand's defense against counterfeiting.

4 WAYS TO PROTECT YOUR BRAND

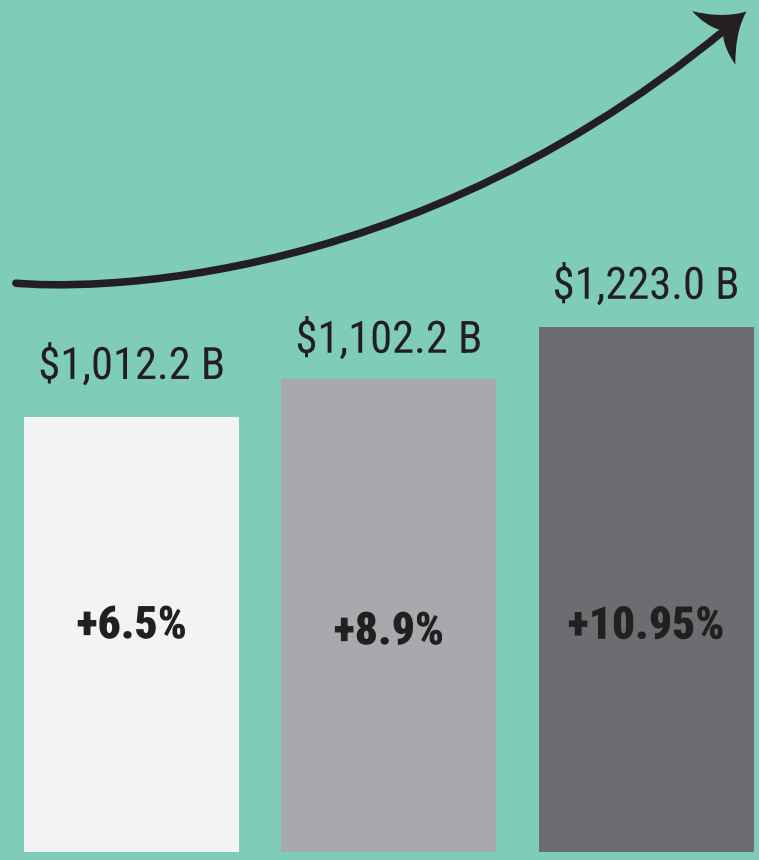


BrandShield®

With U.S. sales expected to reach more than 1.2 billion in 2024, the holiday season presents a perfect opportunity for counterfeiters to exploit the surge in online shopping. There is no question that with spending at a peak, scammers are exploiting this increase to deploy counterfeit goods, phishing schemes, fake websites, and other tactics to deceive consumers and undermine brand trust and loyalty.

By taking proactive steps—such as implementing a digital risk protection tool, and taking action in real time, brands can better protect themselves against these threats. Early action can be key; starting to monitor and use protective measures well before the holiday season not only helps identify risks but also provides the time needed to address them effectively. As counterfeiters evolve their tactics, staying vigilant and adopting a digital risk protection strategy is essential for safeguarding your brand's reputation, protecting customers, and securing long-term loyalty in the competitive holiday shopping landscape.

Brands need to make sure the holiday cheer this year isn't overshadowed by fraud—act now to protect your brand and keep your customers trust.



https://www.sellerscommerce.com/blog/us-ecommerce-sales/

Happy Holidays!