



BOARDROOM

INSIDER COMMUNITY



Protecting brand and revenue:

Reducing bots and abuse across
the customer journey

Foreword

Does it feel like scrapers have become a big problem lately? It's not your imagination. Post-COVID, scraper bots targeting retailers have become more evasive – and sophisticated – as they harvest data to exploit and monetise at your brand's expense.

But many leaders are unaware of, or underestimate, the damaging impacts scraper bots can have on website performance, data security and company revenue. While SEO scraper bots can be beneficial to driving search rankings and discoverability, scraper bots with more nefarious intentions are being deployed to undercut your pricing, scalp limited inventory and create counterfeit sites aimed at stealing customer information. That's why greater awareness – and collaboration across digital, marketing, fraud and security teams – is needed to not only protect the brand, but also the bottom line.

This report illuminates why removing scrapers from your website will have positive impacts across many facets of your retail organisation. You can't defend against what you can't see. With the scrapers gone, you'll be better prepared to maximise your revenue potential – and optimise your customer's path to purchase.

Susan McReynolds

Global Industry Strategist, Commerce, at Akamai



Introduction

Bot attacks targeting retailers are on the rise. Phishing campaigns targeting retailers are also on the rise. Collectively, scraping, loyalty and payment card fraud saw an uptick of over [700%](#) in the second half of 2023. Sixty percent of ecommerce merchants and 53% of retailers experienced a [surge](#) in overall fraud levels. Digital channels accounted for [52%](#) of overall fraud losses in the EMEA region, surpassing physical fraud for the first time due to the anonymity of digital transactions.

The result? Last year, losses from fraudulent retail activity across EMEA were increasing across the board, amounting to [£11.3 billion](#) in the UK and [€15 billion](#) in Spain. [Ninety-four percent](#) of online stores in Germany were affected by fraud, with 20% of them experiencing losses of over €100,000.

This isn't just a security issue – an IT challenge for CTOs and CIOs to solve. This is a business optimisation problem. For retail brand and marketing leaders in particular, online abuse can skew product data, website and engagement traffic, impacting strategy and budgets, as well as hard-won reputation and trust. And the impact on growth can be devastating.

This is a business-critical challenge, with the same end goal of enhancing the customer journey and increasing their loyalty. In this new era of online fraud, teams must break down silos and work cross-functionally to address it.


As [Susan McReynolds, Global Industry Strategist, Commerce, at Akamai](#), states, *“Tackling and protecting the customer journey, protecting your profits, protecting the brand and revenue, requires everyone to understand the impact all along the way of that order lifecycle.”*

This report outlines:

- How the pandemic changed the nature of digital threats within retail
- Why retailers must act now
- Current and emerging fraud trends
- Their impact on brand and revenue
- How to tackle these challenges



Section 1: How bots have changed – and why it matters

 During the COVID-19 pandemic, increased reliance on digital platforms (both from a business and consumer perspective) led to a host of new vulnerabilities, fundamentally reshaping the landscape of retail fraud. How? Attackers follow money. And during the pandemic, that money shifted more online than ever before.

The unprecedented demand for certain products such as toilet paper, sanitisers, baby formula and home workout equipment created lucrative opportunities for bot operators to exploit these conditions. [Scraper bots](#), for instance, hoarded high-demand items only to resell them at inflated prices, capitalising on shortages and high consumer demand.

Up until this point, scraper bots weren't causing significant widespread damage and were quite noticeable. This therefore rendered them easier to tackle with traditional security tools. But as they were the first step in an inventory hoarding attack, and this hoarding was so profitable, bot operators decided to invest significant resources into making scrapers more evasive.

At the same time, advancements in machine learning and AI created a perfect storm for attackers to achieve their goal. It also increased the ability to launch multiple attacks at once, using sophisticated evasion techniques, like rotating IP addresses and proxies, to bypass traditional bot detection systems. As [Richard Meeus, Director of Security Technology and Strategy EMEA at Akamai](#), outlined, *"Bots are becoming increasingly clever. They can exactly mimic a human being, and can zip in and zip out before you've even seen them, making them harder to detect and combat. They're also coming in at huge volumes, from thousands of different places. No retailer is immune."*

The astronomical rise in online transactions caused by the pandemic (global online retail sales' share of total retail sales grew on average from 16% to [19%](#) in 2020) also saw an increase in more direct forms of fraud, such as account takeover (ATO) and phishing attacks designed to steal sensitive information. Retailers faced challenges in distinguishing between legitimate customer interactions and malicious bot activities – and malevolent actors exploited those weaknesses in the retail tech stack.

Unfortunately, these susceptibilities remain. Retailers are struggling to keep pace with the evolution of digital fraud and abuse, which is snowballing faster than ever. And with the growth of global ecommerce – roughly 22% of global retail sales in 2024, projected to grow to [27%](#) by 2026 – the onus is on retailers to protect the increasing amount of legitimate customers shopping online.

Section 2: How malicious activities reduce retail revenue and erode consumer trust

The impact of malicious activities on retailers fundamentally affects the bottom line. One recent [study](#) found that merchants incur an average **cost of \$3 for every \$1 of fraud**. The latest [figures](#) from 2023 indicate that the total cost of ecommerce fraud globally **exceeds \$48 billion**, up from **\$41 billion in 2022**. Cumulative [losses](#) to online payment fraud globally will climb to over **\$343 billion**. To put this in perspective, that's more than three times Apple's net income in 2023.

And that's just the obvious financial impact – there's still an unaccounted (and arguably substantially more costly) value to losing competitive advantage, eroding brand value, loyalty and trust. So how and where does that manifest in the business?



The role of scraping in undermining pricing strategies and exclusivity

Scraping, the practice of extracting data from websites using automated bots, poses a significant threat to retailers' brands, pricing strategies and product exclusivity. And for many retail organisations, they don't even know that they have a scraping problem – or even worse, they don't realise the true impact this type of activity has on the business.

Here are six ways scraping can hurt your business:

1. Price monitoring and undercutting

Competitors can use scraping bots to continuously monitor a retailer's pricing information. With this data, they can undercut the retailer's prices, making it challenging to maintain a competitive advantage or implement dynamic pricing strategies effectively.

2. Competitive disadvantage

Drilling deeper into this point, the scraping of pricing, product and inventory data allows competitors to gain valuable insights into a retailer's strategies, enabling them to adjust their own tactics accordingly and gain an unfair advantage. The playing field is no longer level.

3. Loss of exclusivity and brand value

You know the blood, sweat and tears your marketing team put into creating product images and descriptions? Scraping bots can extract them and other proprietary content from a retailer's website. This stolen content can then be used to create counterfeit or unauthorised listings on third-party marketplaces or even look-alike websites, undermining exclusivity and brand value.

At a larger level, this is a brand impersonation issue. Some of the resellers are not malicious, but many of them are, setting up these pages purely to steal credit card information. And your consumer doesn't know the difference.

4. Inventory hoarding

Bots can scrape real-time inventory data and bypass purchase limits or queue

systems, giving them an unfair advantage over human customers; as previously mentioned, this allows resellers or scalpers to hoard limited-edition or big hype items, such as PlayStations, beauty brands or shoe drops, leaving legitimate customers unable to make purchases. Even if they can, many of these resellers will mark up the price by 3x or more, leading to upset from loyal customers.

5. Inaccurate inventory levels

Bots that hoard or purchase large quantities of products can rapidly deplete inventory levels, leading to stockouts (and disappointed customers). This has a further negative effect on sales forecasting.

6. Skewed marketing metrics

These bots act like humans, and your analytics will reflect them as such, skewing your marketing data. For one of Akamai's customers, 90% of their traffic ended up being bots, which had a major impact on their marketing campaigns and cloud costs.

As Christine Ross, Product Marketing Director at Akamai, outlined: "Customers have told us, 'This product gets pinged on my website all the time. It must be a really popular product', but it's actually the bots that are looking at it and not humans. So they bought more of a particular product because the website said it was popular, but in fact, people weren't buying that. People weren't checking out that page. These impact major inventory and website optimisation decisions. And sometimes, if you don't pull the bot data out of it, then you're optimising for the bots and not for consumers. This can eradicate marketing ROI and hamper business growth."



Diminished site performance and its repercussions on user engagement

Another area that takes a major hit is website performance, a retailer's window to the world. Bots performing scraping or inventory hoarding can overload a retailer's website infrastructure, leading to slower load times, increased server costs and even site outages. This degradation in performance directly impacts user engagement, as customers faced with slow-loading pages or downtime are likely to abandon the site, potentially turning to competitors.

Given the fact that the average page views per buying session stretched beyond 20 pages in 2023, outlining the necessity of more pages and content for conversion, a highly performing website becomes all the more crucial. User frustration with retail websites is real and it's rife, affecting [40%](#) of shopper experiences. This directly correlates to conversion – and costs retailers nearly \$0.60 per visit in wasted spend.

Poor user experience is also the enemy of retention. Returning customers convert four times more than new ones and are less likely to come from paid channels. If you're a marketing leader juggling a tightening budget, this is a key point of note.

Compromised accounts and the associated financial and reputational costs

Bot-driven credential stuffing attacks and phishing campaigns can lead to compromised customer accounts, which are particularly damaging. These stolen credentials can then be used for account takeover, identity theft or even data breaches – all of which affect customers' finances and security, with the blame landing squarely on your doorstep.

From a retailer perspective, unauthorised account access can immediately lead to fraudulent orders and chargebacks, loyalty point theft, coupon/promotion abuse, the resale of accounts and CVV validation attacks – to name a few. The long-tail fallout of account takeover can include asset replacement for customers, potential fines, diminished brand trust, increased fraud investigation costs and burnout across fraud, security and marketing teams.

With respect to data breaches, the financial costs to address remediation include:



Increased operational costs

(e.g., security, compliance, or even, as with [Neiman Marcus](#) in 2021, setting up a dedicated call centre to field customer complaints as to how they were affected).



Refunds and credit monitoring services

for affected customers (an example of this includes Hudson Bay in 2018 offering breached customers identity protection services).



Legal fees and settlements

After a 2013 [breach](#) of payment card information, retail giant Target had to settle a series of lawsuits, totalling nearly [\\$300 million](#). The impact on their growth was severe: Target's profits fell almost 50% in Q4 of that year compared to the prior year and its stock price fell 9% over a period of two months following.



Regulatory fines and investigations

In the case of Target, the Justice Department launched an investigation. When [Dixons Carphone](#) had 14 million customers' information compromised in 2018, the Information Commissioner's Office fined them the maximum penalty of £500,000.




The reputational costs of compromised accounts and breaches also impact overall growth. [Fifty-four percent](#) of customers say they would switch to a different brand if the one they used experienced a data breach. For publicly traded companies, they suffer an average loss of [3.5%](#) on their share price after a breach. In the case of Dixons Carphone, declining profits led to the closure of 100 Carphone Warehouse stores within a year and the entirety of the Carphone Warehouse brand by 2020.

Compromised accounts are a significant factor in customer perception, trust and loyalty, which sit at the core of every brand and marketing leader's objectives. For instance, Target's consumer perception pre-breach sat at [20.7](#) on the Brand Index Buzz rating, plummeting to a low of 9.4 the year after. Five years later, the number was at 17.3, outlining the mountain they had to climb to regain their standing amongst consumers. In today's connected, social media-saturated environment, brand perception can be made or broken in minutes.

Changing consumer behaviour coupled with the cost of living crisis has also upended consumer loyalty. Trust, a gateway to loyalty, is key to winning the next generation of consumers and fostering sustainable business growth. Millennials and Gen Z have the lowest [levels](#) of brand trust, perhaps attributed to the fact that roughly [20%](#) of them have had their data knowingly compromised (in comparison to 2% of Gen X and 10% of Baby Boomers).

Therefore, this trust-building requires fast, frictionless and fraud-free experiences. Shoppers are willing to pay 46% more with a retailer they trust. The highest factor to achieving that trust? A secure checkout process and protection of personal data. A global 2023 [study](#) outlines that nearly 90% of consumers state that this is vital for retailers to accomplish that goal. Strong brand reputation also made the top list, with 76%.

Conclusion: Combating bots and abuse via organisational alignment

 Given the increasing rampantness of these malicious technologies, this can feel like yet another mountainous challenge to tackle. But it doesn't have to be. The good news is that there are effective ways to keep your brand within your control and enhance your customer journey. But where to start?

Strategies for protecting your brand – and your bottom line

It's no surprise that different teams are usually focused on protecting different outcomes: security protects data, marketing protects revenue, IT protects against outages, CX protects the customer path to purchase. But these teams have several challenges to tackle:

- *Are they communicating and on the same page about shared business outcomes and goals?*
- *Can they answer the question “Are stakeholders aligned on the technical requirements and tools to protect customer data, the brand and revenue?”*

Most of the time we find that the answer is no. But this is critical. Further key questions these teams need to collectively answer include:

- *What are the outcomes we are trying to achieve (e.g., protecting revenue, customer data, the path to purchase, fraud)?*
- *Do we need one solution or multiple solutions to solve various stakeholder challenges and use cases?*
- *Is there a disconnect between who is buying the solution and who is actually using it?*
- *What does success look like? Do we have clearly defined KPIs?*
- *What are we willing to tolerate/what trade-offs have to be made to balance security with the need to optimise the path to purchase?*
- *Are we protecting our entire estate (website, mobile app, APIs and infrastructure)?*
- *How do we handle the desired, undesired and the fuzzy frontier between the two?*

 **Every team needs to understand these points and have a shared goal that drives alignment and action for optimal outcomes for the business.**

Retail fraud is accelerating at an enormous pace and having widespread impact on retailers. As we've outlined, the losses go beyond those easily seen on a ledger from fines, settlements or legal fees. They strike at the heart of the ultimate retailer objective of driving revenue through brand and customer loyalty. Brand and loyalty rely on trust and customer experience – factors diminished in a blink of an eye through fraudulent activity.

The increase in abuse, coupled with a difficult consumer buying landscape and the steady climb of online sales, means it's more vital than ever for retailers to prioritise and invest in advanced security measures to protect their brand and customers. This means business units must work together to understand and share the impact of malicious attacks, as they are no longer the realm of security and IT teams alone.

If you need support, [get in touch with the Akamai team](#) or learn more about [retail, travel and hospitality solutions](#). Akamai has been [helping global retailers and brands](#) such as [Lufthansa](#), [Wagner eCommerce Group](#), [Panasonic](#) and [TOUS](#) deliver safe and engaging online experiences for more than 25 years.



About Akamai

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. [Akamai Connected Cloud](#), a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's cloud computing, security, and content delivery solutions at [akamai.com](#) and [akamai.com/blog](#), or follow Akamai Technologies on [X](#), formerly known as Twitter, and [LinkedIn](#).



This paper was brought to you in conjunction with Retail Gazette, the UK's largest B2B retail publication.

Visit [www.retailgazette.co.uk](#) to join 300,000 other monthly users for free to access to the latest news, interviews, analysis, in-depth reports and white papers.

