Black Friday & Cyber Monday: A Data-Driven Report for eCommerce

SEON

Table of Contents

Introduction 3

Data Methodology & Disclaimer 4

Attack Vectors & Behavior Shifts 5

Fraud Impact on Customer Experience & Operations 7

Regional Fraud Patterns in Peak Season 9

How to Prepare for Black Friday & Cyber Monday Fraud Surge 10

November Readiness Checklist 11

Key Takeaways 12

About SEON 13

Introduction

Black Friday and Cyber Monday are bigger than strictly sales events; they are stress tests for every retailer's fraud prevention strategy. SEON's analysis of October to December 2024 data from eCommerce leaders, Buy Now, Pay Later (BNPL) providers, gateways and payment service providers (PSP) shows that **fraudulent transactions ran approximately five times higher on Black Friday and more than four times higher on Cyber Monday compared to October baselines.**

This surge was not simply the byproduct of higher shopping volume. Fraud volumes rose far faster than overall traffic. Due to the huge volume, rates held flat-to-down at a weekly level, but day-level rates and intervention intensity spiked around Black Friday and Cyber Monday. Bad actors frequently used coordinated, bot-driven account takeovers, synthetic identities and VPN masking to blend into legitimate traffic and maximize payout.

This report unpacks how fraudsters escalated attacks during Q4 2024, focusing on volume, rates and behavioral shifts. It then distills insights into an actionable playbook so merchants can protect revenue, maintain customer trust and keep checkout friction low when it matters most.

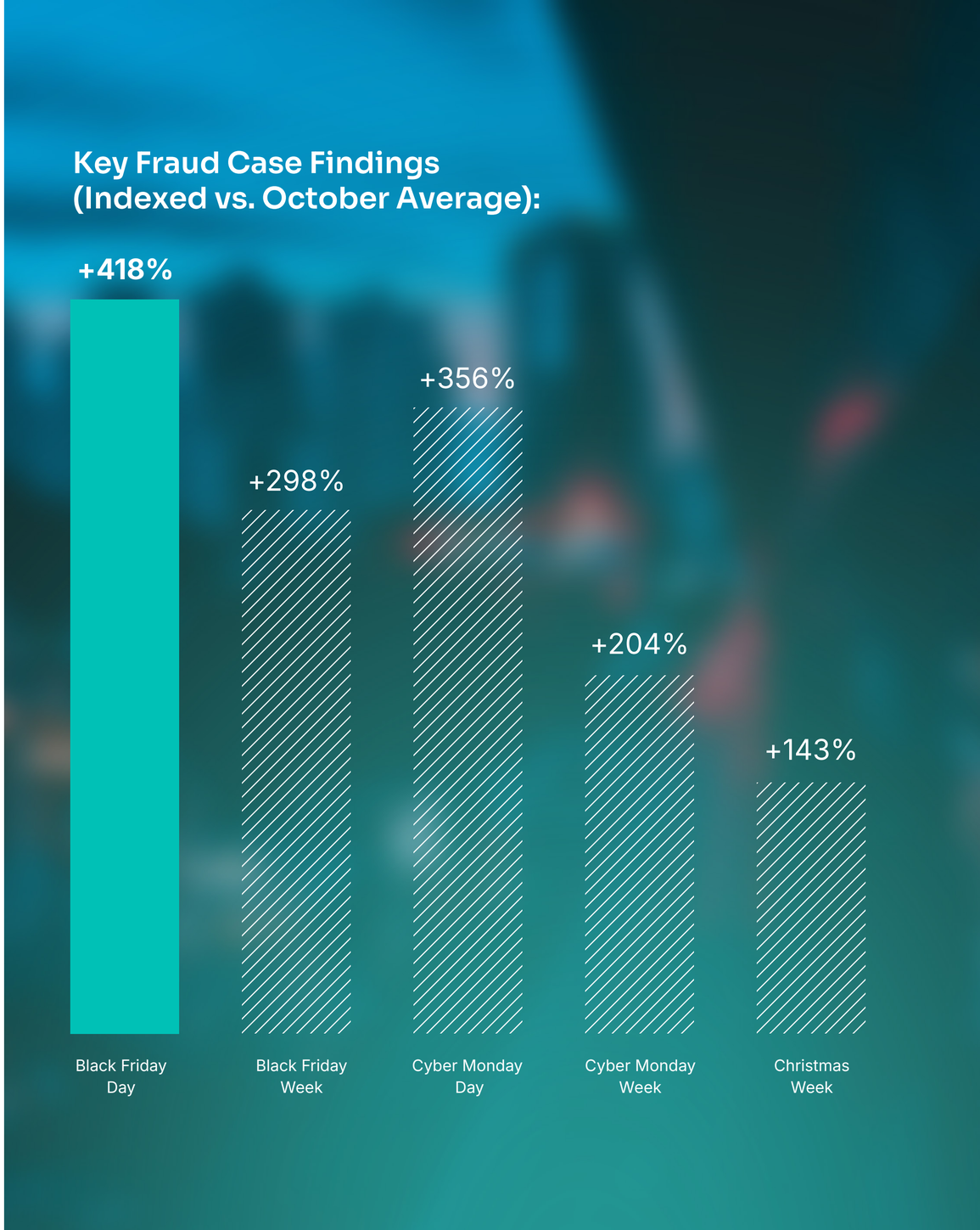
Data Methodology & Disclaimer

This report uses SEON's aggregated October–December 2024 dataset. For clarity, we define:

→ **Black Friday Week, Cyber Monday Week, Christmas Week:** Monday–Sunday windows.

→ **Black Friday, Cyber Monday, Christmas Day:** Single calendar days.

Unless otherwise noted, all percentages represent the lift versus October weeks as a baseline for the same subvertical and region. Counts and rates are weighted by transaction volume where applicable.



Attack Vectors & Behavior Shifts

Fraud last year was highly automated and coordinated — and the data shows how attackers scaled their efforts dramatically.

→ **Bot attacks** spiked 407% during Black Friday Week, remained elevated Cyber Monday Week (+349%) and surged even higher during Christmas Week (+526%), targeting login and checkout endpoints. These attacks focused on credential stuffing, using stolen username-password combos to break into accounts, and automated card testing, where bots quickly run stolen card numbers through checkout pages to find the ones that still work.

→ **Device anomalies**, such as mismatched or manipulated device fingerprints, including spoofed OS/browser settings, emulated hardware (software that mimics the behavior of physical hardware) or IP/timezone inconsistencies, nearly tripled during Black Friday Week (+283%) and spiked again at Christmas (+342%), reflecting widespread use of spoofed devices, emulators and virtual machines to bypass fingerprinting.

→ **Newly created email addresses** rose by +35% during peak weeks (Black Friday and Cyber Monday) and more than doubled during Christmas Week (+115%), signaling synthetic identity creation and promo abuse campaigns.

→ **VPN usage** remained flat or slightly down, while suspicious browsers dropped sharply (–56% to –79%), suggesting attackers now use real browsers, which are harder to flag than automated ones, and clean IPs (residential or trusted networks) to better blend in with legitimate users.

→ While not separately quantified, **transaction monitoring data** shows clusters of rapid, low-value purchases consistent with stolen card testing and credential stuffing.

These trends indicated that fraudsters were less likely to hide behind VPNs or obviously fake browsers. Instead, they act like real shoppers, using standard internet connections, real browsers and spoofed devices to appear more legitimate. This shift makes them harder to spot, so merchants must check many signals simultaneously to catch attacks before they cause significant losses.

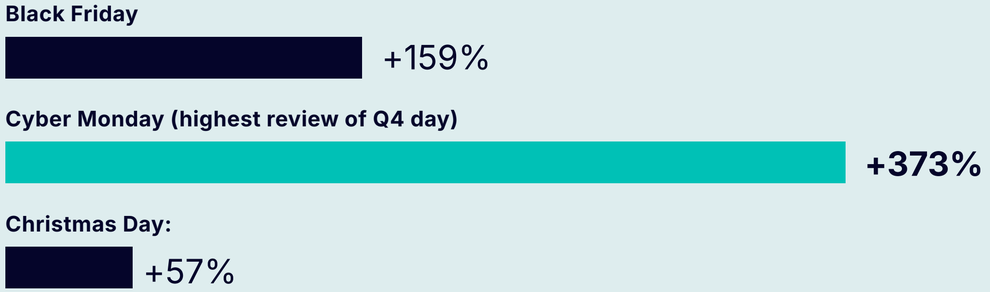
Together, these findings confirm that this is not opportunistic fraud; it is coordinated, disciplined and scaled to match holiday demand. Merchants relying only on static rules risk letting these patterns slip through until the financial damage is done.

Fraud Impact on Customer Experience & Operations

The Q4 fraud surge didn't just strain detection systems; it put heavy pressure on fraud operations teams and risked frustrating legitimate customers. While fraud was stopped effectively, the interventions came at the cost of time, resources and conversion rates.

Manual Review Workload Surged (Indexed vs. October Average):

More fraud attempts meant fraud teams had to perform significantly more manual reviews during Black Friday and Cyber Monday fraud spikes, which slowed down real customers. On a typical day, teams conducted **121 reviews per day (baseline)**, but on peak days, workloads spiked:



Manual reviews on Cyber Monday were up +373% — the single highest day in Q4 — despite a lower weekly fraud rate. That's where revenue gets squeezed: more friction, same fraud rate.

This surge reflects the flood of borderline transactions that couldn't be automatically approved or declined, forcing analyst intervention. Without automation, queues like these slow fulfillment and drive up operating costs during the most revenue-critical weeks of the year.

Fraud Rate Stayed Flat-to-Down

Weekly fraud rates stayed flat-to-down (Cyber Monday Week: 3.30% vs. 4.06% “Other” weeks), meaning more legitimate transactions were flagged and delayed.

Conversion Risk from Friction

The combination of elevated review rates and fraud controls meant more step-up authentication and verification challenges. On Cyber Monday, when review volumes were up +373%, each additional step introduced potential friction at checkout. This represents a heightened risk of cart abandonment, a costly possibility when traffic and purchase intent are at their highest.

Why It Matters

Operationally, this data section shows merchants can win the fraud fight but lose revenue if review queues slow fulfillment or friction drives away legitimate customers. Automation, risk-based decisioning and dynamic friction are essential to keep genuine transactions flowing without overwhelming fraud teams.

Regional Fraud Patterns in Peak Season

Fraud patterns were not uniform across regions or payment types, and the data highlights where risk was concentrated. The most severe fraud exposure during the 2024 peak holiday period centered on eCommerce, as detailed in Section 1.

Regional Hotspots

Regional weighting of risk vectors shows that the US and select Western European markets contributed the highest share of bot activity, device anomalies and newly created emails:

- → **Bots:** Majority of +407% Black Friday Week spike driven by US/EU traffic
- → **Device Anomalies:** +283% Black Friday Week, with the heaviest concentration across select Western European markets
- → **New Emails:** +35% Black Friday/Cyber Monday Weeks, with the US contributing highest proportion of flagged sign-ups

Concentrations aligned with where shopping demand and fraud opportunity were highest. Fraudsters follow peak promotional traffic, using the US and Western Europe as regional fraud hotspots for bot attacks, card testing and promo abuse.

These data points confirm that fraud operations must prioritize where the risk is heaviest. Direct eCommerce channels and specific US/EU geographies carry the highest exposure and should receive more aggressive controls, velocity monitoring and preemptive tuning ahead of peak shopping weeks.

How to Prepare for Black Friday & Cyber Monday Fraud Surge

Fraud prevention during Q4 cannot be a one-day effort. Instead, it must be treated as a sustained campaign. The data shows that fraud activity begins ramping in early November and persists through Christmas Week, meaning merchants need proactive, adaptive measures that scale across the entire season.

November Readiness Checklist

1 Start Early

Tune rules and machine learning models early to catch early fraud tests.

Monitor new email creation rates and device anomalies for signs of coordinated attack prep.

2 Layer Signals

Combine device, email, IP and behavioral analytics for a holistic risk view.

Cross-reference returning devices and accounts to catch fraud rings operating across weeks.

3 Automate Decisioning & Reviews

Use automated case routing and labeling to keep queues manageable.

Prioritize the riskiest transactions for analyst attention to minimize review backlogs.

4 Deploy Dynamic Friction

Step up only where risk scores exceed defined thresholds to preserve conversion.

Offer alternative verification methods (e.g., email or SMS confirmation) to reduce customer drop-off.

5 Track and Block Repeat Offenders

Maintain and share blocklists of known bad devices, IPs and emails across promotional periods.

Use velocity rules to detect rapid repeat attempts from the same source.

Retailers that execute this plan can absorb the holiday fraud surge without overloading fraud teams or alienating customers. By treating fraud and risk prevention as a multi-week campaign, merchants turn a peak-season risk into an opportunity to capture more good revenue.

Key Takeaways

Peak-season fraud isn't a single-day challenge; it's a sustained campaign that requires strategic preparation. Our October–December 2024 analysis shows that attackers scaled efforts across entire weeks, targeting eCommerce checkouts with automation and device spoofing. These key takeaways summarize where risk was concentrated and how merchants can stay ahead in 2025.

- → **Fraud is a Multi-Week Campaign:** Black Friday and Cyber Monday are not isolated spikes; fraud risk stayed elevated across both weeks, resurging at Christmas.
- → **Automation Drives Scale:** Bots (+407% BF Week) and device spoofing (+283%) dominated attacker tactics, proving fraud is coordinated and industrialized.
- → **Manual Review Strain Threatens CX:** Cyber Monday reviews surged +373% despite lower fraud rates, signaling friction for good customers and potential lost revenue.
- → **Targeted Defense Wins:** eCommerce and US/EU traffic carry the highest exposure, making them the priority for layered, dynamic defenses.

Peak-season fraud is an arms race, and merchants that treat prevention as a strategic capability, not a reaction, have the advantage. The data shows that attackers are disciplined, precisely timing campaigns and scaling them to match retail demand. The next phase of fraud strategy is about anticipation: using insight, automation and agility to stay one step ahead, turning the busiest quarter of the year into the most profitable.

Book Your Holiday Fraud Readiness Review with SEON

Schedule a readiness session with SEON’s fraud experts to stress-test your defenses now. Don’t wait until Black Friday to find the gaps.

Speak with an Expert

SEON

About SEON

SEON is the command center for fraud prevention and AML compliance, helping thousands of companies worldwide stop fraud, reduce risk and protect revenue. Powered by 900+ real-time, first-party data signals, SEON enriches customer profiles, flags suspicious behavior and streamlines compliance workflows. With integrated fraud and AML capabilities, SEON operates globally from Austin, London, Budapest and Singapore.

Learn more at seon.io