

PEAK SEASON PLAYBOOK

How not to spend Black Friday rebuilding your product catalog

What every Shopify merchant needs to sort before the season starts.

What it actually costs when things go wrong

Black Friday and Cyber Monday are the most high-stakes 96 hours of your year. Here's what the math looks like when something breaks.

BFCM accounts for roughly 4% of your annual revenue compressed into four days. For a \$20 million store, every hour during that window is worth approximately **\$8,000** in direct revenue.

THE BFCM MATH FOR A \$20M STORE

YOUR STORE

\$20M

annual revenue

BFCM SHARE

~4%

earned in 96 hours

WEEKEND HOURS

96

across the weekend

÷

=

HOURLY EXPOSURE

\$8,000

lost for every hour your store is offline or broken

Source: Shopify BFCM 2025 Data Report (\$14.6B over 96 hrs); Shopify 2025 Annual Report (GMV \$378B). 3.86% applied to a \$20M store yields ~\$772K BFCM revenue. $\$772K \div 96 \text{ hrs} = \sim\$8,000/\text{hr}$.

The real risk isn't Shopify going down

It's something in your store breaking while Shopify's status page stays green: a bad bulk import, an app misfire, an AI tool deleting variants at scale. Quieter than an outage. **Identical revenue impact.**

This playbook is organized around five questions every merchant should be able to answer before the season starts.

01 What are you actually responsible for protecting?

Section 1 · The ownership gap

02 What are the most likely failure modes, and how do they change at BFCM?

Section 2 · The eight ways data disappears

03 Are you ready?

Section 3 · A 25-point prep checklist to find out

04 If something breaks at 11pm on Black Friday, what do you do?

Section 4 · A recovery playbook for peak season

05 How do you build a store that bounces back fast?

Section 5 · Four practices for a resilient store

The ownership gap: what Shopify covers, what you cover

Shopify is a well-run, reliable platform. But understanding what it covers and what it does not is the thing most merchants only figure out after something goes wrong.

SHOPIFY OWNS

The infrastructure: servers, CDN, uptime, and payment rails.

YOU OWN

The data inside your store: every product, variant, image, collection, order, customer profile, metafield, theme, and page.

Shopify operates under a **Shared Responsibility Model**, and its Terms of Service state this explicitly. What surprises merchants is the practical implication: Shopify provides no merchant-controlled backup, no point-in-time restore, and no way to recover a deleted product with its images, metafields, and variants intact.

Who owns each category of your store data

DATA CATEGORY	WHAT IT INCLUDES	OWNER
Platform infrastructure	Servers, CDN, payment rails, fraud detection, uptime	Shopify
Products & variants	SKUs, prices, descriptions, images, metafields, inventory	You
Collections & tags	Collection rules, sorting, product assignments	You
Themes & customizations	Theme code, custom sections, settings	You
Customer records	Contact data, order history, loyalty tier, tags	You
Order data	Order details, fulfillment status, custom attributes	You
Metafields & metaobjects	Custom data fields, structured content, size charts	You
Pages & blog content	Landing pages, buying guides, blog posts	You

Closing the gap requires a backup solution that operates **outside Shopify's infrastructure** and restores specific items without touching anything that is still intact.

The green status page problem

The data incidents most likely to affect revenue during BFCM will not trigger a Shopify status page alert. A bad CSV import, a misprompted AI tool, or an app that corrupts product variants on install will not show up anywhere except in your own store. By the time customers notice, the incident may have been running for hours.

● Shopify status

All systems operational. Nothing here will warn you about what's happening inside your store.

● Your catalog

Variants silently overwritten by a bad import. Sales falling. No alert anywhere but your own dashboards.

"I chose to work with a company like Rewind for the nuclear saving, knowing that whatever happens, we can get it back."

FOUNDER • 7-FIGURE DTC TRAVEL ACCESSORIES BRAND

SECTION 2

Eight ways store data breaks, and why each costs more during BFCM

Most data incidents don't look like disasters. They look like a bad import, a misconfigured app, or a team member who made a mistake. During BFCM, every one of them costs more, and none are recoverable through Shopify's native tools.

01

EVERYDAY

Human error: accidental delete

The most common incident. A team member deletes a product, removes a collection, or clears a set of metafields. No malice intended.

BFCM amplifier: more hands on deck, more urgency, more mistakes.

02

EVERYDAY

Bad bulk import or export

An incorrectly formatted CSV is uploaded. Prices are overwritten across hundreds of products, variants erased. The change propagates instantly.

BFCM amplifier: catalog updates are frequent pre-BFCM.

03

COMMON

Integration sync error

A connector between Shopify and your ERP, PIM, or inventory system pushes bad data. Product records are overwritten with stale or incorrect information.

BFCM amplifier: inventory sync volume spikes sharply.

04

ACCELERATING

AI automation misfire

An AI tool or automated workflow is misprompted and executes a bulk change across your catalog. The window between command and damage is seconds.

BFCM amplifier: teams lean heavily on AI during prep.

SECTION 2 • THE REMAINING FOUR

05

HAPPENS

App deletes data on install or removal

An app modifies or removes metafields, tags, or product data when installed, updated, or uninstalled. Often undocumented behavior.

BFCM amplifier: teams install promotional apps just before launch.

06

HAPPENS

Agency or contractor overwrites your catalog

A freelancer or agency with admin access runs a bulk operation that wasn't scoped correctly. Entire product categories are affected.

BFCM amplifier: external help is brought in for seasonal prep.

07

RARE

Account breach or unauthorized access

A compromised credential gives an unauthorized party admin access. Product data, customer records, or pricing can be altered or deleted.

BFCM amplifier: higher-value target during peak revenue.

08

RARE

Theme or app deploy breaks the storefront

A theme update or app code change causes checkout errors or broken product pages. Revenue stops even though the data is intact.

BFCM amplifier: zero-tolerance window for storefront errors.

Recovery time is the real cost metric. Every hour of manual rebuild is an hour of lost BFCM revenue.

"We had an inadvertent loss of all of our product variants through a Shopify import. It was just an incorrectly formatted CSV file."

ECOMMERCE MANAGER
ENTERPRISE FOOTWEAR BRAND

"If it takes us a day to repopulate from our systems versus two hours from yours, well, that's 22 hours of revenue."

ENGINEERING LEAD
ENTERPRISE APPAREL BRAND

SECTION 3

The BFCM prep checklist

Twenty-five checks across five areas. Work through this at least two weeks before your campaigns go live. Anything you can't check off today is your action list.

AREA 1 • BACKUP COVERAGE & VERIFICATION

- ☐ Automated backups are running and confirmed current · verify the last successful backup timestamp.
- ☐ Backup covers every BFCM-relevant data type: products, variants, metafields, collections, pricing, themes, and customer records.
- ☐ You've tested a restore in the past 90 days · you know how long a full catalog restore takes and verified the data looked correct.
- ☐ Backup storage is independent of Shopify's infrastructure · accessible even during an account-level issue.
- ☐ You have a 1-year-or-longer retention policy · restore to any point in the past year, not just the latest version.

AREA 2 • MONITORING & ALERTING

- ☐ Real-time alerting for bulk product changes · you're notified before a bad import or AI automation spreads.
- ☐ Checkout flow is monitored with simulated transactions · you find out about a failure before your customers do.
- ☐ Third-party app monitoring is active · if a key app (loyalty, reviews, upsell) goes down, your team gets an alert.
- ☐ Alerts route to the right people · your on-call contact gets them on phone or Slack, not in an unmonitored inbox.
- ☐ GA4 / key metrics watched for anomalies · a sudden drop in add-to-cart rate signals a broken page or checkout.

SECTION 3 • CHECKLIST, CONTINUED

AREA 3 • STAGING & PRE-LAUNCH TESTING

- ☐ All BFCM theme changes tested in staging against current production data, not a weeks-old snapshot.
- ☐ Any new BFCM apps (promotions, countdown timers, upsells) tested in staging before going live.
- ☐ Discount codes, automatic discounts, and pricing rules tested end-to-end · checkout completes with BFCM pricing.
- ☐ Bulk catalog changes tested on a small sample in staging before running against the full catalog.
- ☐ Staging is synced to production · you're testing against current data, not stale catalog information.

AREA 4 • ACCESS CONTROL & TEAM PREP

- ☐ Admin access audited · anyone who no longer works with your store, including past freelancers, has been removed.
- ☐ Team knows not to run bulk imports without an on-demand backup first and sign-off from a lead.
- ☐ On-call coverage is defined · a named person can make recovery decisions at any hour during the peak window.
- ☐ Vendor and agency access is scoped to the minimum permissions needed · not full admin.
- ☐ At least two people have practiced a restore · no one is reading documentation at 11pm.

AREA 5 • DATA INTEGRITY PRE-LAUNCH

- ☐ All BFCM pricing reviewed and confirmed · no products showing original prices where discounts should apply.
- ☐ Inventory levels reconciled against your warehouse or 3PL · zero-inventory variants set correctly.
- ☐ Metafields for specs, size charts, or custom content spot-checked across your top BFCM SKUs.
- ☐ All BFCM collection pages reviewed in a real browser · products, sort order, and rules correct.
- ☐ A final on-demand backup taken after all changes and before launch · your known-good restore point.

When something breaks: a recovery playbook for peak season

Speed matters. Every minute between incident and recovery is revenue. This section is designed to be usable at 2am. Confirm scope before acting. These steps apply whether you discover the incident from an alert, a customer complaint, or your own team.

STEP 1 • IDENTIFY & CONTAIN

- 1 Confirm the scope before acting** 2 min
What is affected: specific products, a collection, a theme section, or the whole catalog? Use your backup tool's audit log to identify what happened.
- 2 Stop the source of the problem** 5 min
Disable the app, cancel the running import, or revoke access temporarily. Stopping the cause prevents more damage while you recover.
- 3 Take an on-demand backup before restoring** 2 min
Even in a corrupted state, snapshot first. It preserves the incident for investigation and ensures your restore does not affect data that is still intact.

STEP 2 • RESTORE

- 4 Choose item-level restore whenever possible** 3 min
If the incident is scoped, restore only what was lost: the affected products, metafields, or theme section, without touching anything that is still working.
- 5 Use version comparison to pick the right restore point** 2 min
Verify the restore point contains correct data before you commit. Restoring to a version that also had the problem only extends your incident.
- 6 For full-catalog incidents, run a full restore and confirm** 10 to 30 min
Restore from your most recent known-good backup, then spot-check at least 20 products across categories before declaring the store clear.

7

Run a checkout test before declaring recovery complete

5 min

Place a test order with a test payment method. Confirm cart, pricing, and checkout work end-to-end. A restored catalog that cannot convert is not yet a recovered store.

8

Notify your team and log the incident

5 min

Record what happened, when, what was affected, how it was fixed, and estimated impact. The log is how you prevent the same incident next BFCM.

THE PRE-BFCM DRILL

Practice the playbook a week before the season

Delete a test product, time your restore, and confirm every team member who might be on call knows how to execute steps 1 through 8.

Minutes

A practiced team recovers in minutes.

Hours

An unpracticed team recovers in hours.

Building a store that bounces back fast with Rewind

Rewind Protection Suite detects, prevents, and reverts unwanted changes before they affect your bottom line, across four modules: Backups, Monitor, Staging, and Alerts.

01 Automated backups and self-serve restores

REWIND BACKUPS

Recover your store data from automated, comprehensive, daily and real-time backups. The foundation everything else builds on.

Backup changes as they happen

Automated daily backups for all your data and real-time backups for products and orders.

Granular, on-demand restores

Restore anything from a single item to your entire store, exactly how you need it.

365-day history

Unlimited storage with a full year of version history to restore from.

02 Catch downtime before it becomes lost revenue

REWIND MONITOR

Actively monitor any impact to your store's performance so you can act swiftly and keep checkouts flowing.

Simulated user journeys

Ensure key flows like checkout are always working as expected, 24/7.

Always-on monitoring

Get notified of outages on third-party apps.

Email & SMS alerts

Get notified of issues by email or SMS so you can act before customers notice.

03 Test and sync store changes with confidence

REWIND STAGING

Safely test changes to themes, apps, and code, then push them live.

Staging made simple

Safely test and QA new updates to your store before going live.

Continuous sync

Maintain up to 10 test stores with continuous sync and automated store copies.

Deploy from staging

Ship store updates or launch in new markets in a few clicks.

04 Stop mistakes as they happen

REWIND ALERTS

Get alerted to bulk changes and set custom thresholds so your product pages stay accurate and live, 24/7.

Bulk change notifications

Real-time alerts on high-volume product changes, so you can revert before sales are hit.

Customizable thresholds

Control how many product changes you consider high-volume.

Change history

Use the in-app list or download a report to see exactly what changed and when.

22 hrs

The difference between recovering a catalog in 2 hours versus 1 day. At a \$20M store during BFCM, those 22 hours represent roughly **\$176,000** in recoverable revenue.

Based on ~\$8,000/hr BFCM revenue for a \$20M store. 22 hours × \$8,000 = \$176,000.



Your store is set for BFCM. Make sure your data is covered.

Set up Rewind in minutes. Automated backups start immediately. No code required.

Get started with Rewind →

25,000+

Organizations protected

7 PB

Data secured

10 yrs

Purpose-built for SaaS

SOC 2 Type II · ISO/IEC 27001:2022 · Shopify Certified Technology
Partner · GDPR · CPRA · CISA Secure by Design · HIPAA BAA
available · DORA Compliant

rewind.com