DELL Technologies

How retailers can reduce fraud risk across in-store and ecommerce channels

Why closing your integration gaps is critical to fraud prevention

Introduction

The retailers growing fastest today share one operational advantage: their systems talk to each other in real time.

When inventory, transactions and devices work as a unified layer across every channel, the result is faster fulfillment, stronger promotional planning, fewer helpdesk calls, and consistent customer experiences from their first location to their fifteenth.

For small and midsize business (SMB) retailers, achieving that level of integration is more attainable than it may initially appear, with immediate benefits to their operations.

These organizations benefit most from systems that function as a cohesive foundation rather than a collection of separate tools.

Dell Technologies provides integrated solutions that align inventory, transaction and device data in real time. What follows is a practical framework for identifying where the system gaps exist in your operation, what it takes to close them and how doing so will help protect your organization against fraud and create measurable improvements across fulfillment, security and growth.

Common forms of omnichannel retail fraud

Retail fraud generally falls into three broad categories, each taking advantage of gaps between systems, policies or device environments.

Return fraud and policy abuse
Timing gaps or inconsistent return policies across online and in-store channels can allow illegitimate returns or refunds to be processed as valid transactions. AI-ready PCs and edge infrastructure from Dell Technologies can detect and flag discrepancies in real time.

Account takeover and cross-channel fraud
Compromised credentials or account misuse across online ordering, in-store pickup, promotion redemption and other touchpoints can appear legitimate when each transaction is evaluated by systems independently.

Device and endpoint vulnerabilities
Unmanaged or inconsistently configured devices such as registers, kiosks or store PCs can introduce exposure by operating outside standard security configurations or device management controls. Hardware-enabled security controls and centralized device management from Dell Technologies help reduce these vulnerabilities.

Three integration seams and what closing them unlocks

The gap	Where it sits	Opportunity unlocked
The inventory seam	Between ecommerce platform and in-store inventory system	Real-time fulfillment accuracy, fewer stockouts, stronger promotional planning
The transaction seam	Between point of sale (POS), ecommerce checkout and customer identity layer	Cross-channel visibility, faster fraud detection, cleaner customer insights
The device seam	Between managed and unmanaged endpoints in the device fleet	Consistent security posture, less IT overhead, faster new-store onboarding

61%

Sixty-one percent of SMB retailers offer BOPIS (buy online, pick up in store).[1]

70%

Seventy percent sell across multiple digital touchpoints simultaneously.[2]

3-5x

Digital sales account for roughly half of their revenue, three to five times the share reported by large mass merchants.[3]

48%

Channel complexity creates real exposure. Return fraud and policy abuse affected 48% of merchants in 2024, and that rate is outpacing most retailers' fraud prevention investment.[4]

SECTION 01

The inventory seam

You can see your inventory report. Can you trust what you see?

When inventory data moves as fast as your transactions, everything gets better. BOPIS orders are more reliable. Promotions run against accurate stock. Returns are processed without manual reconciliation. And the patterns that would otherwise slip through, such as a return processed online and again in-store, get caught automatically.

For a retailer running BOPIS alongside an ecommerce channel and a physical store, that speed isn't a luxury. Every busy Saturday is a test of how well your systems stay aligned under real conditions.

The benefits of closing the inventory seam

Inventory confidence starts with data that's aligned across every channel. When the seam narrows, it:

- Closes the arbitrage window between ecommerce and store inventory.
- Prevents return fraud that exploits delayed inventory updates.
- Reduces stockouts across channels.
- Improves fulfillment accuracy for BOPIS and ship-from-store strategies.
- Strengthens promotional planning with consistent inventory visibility.

How strong is your inventory seam?

Ask your team	What a strong seam looks like
If a customer returns an online order in-store right now, how many places do you have to update manually and what's the window before everything reflects the same inventory?	Updates propagate automatically across all channels within minutes, no manual reconciliation needed.
During your last major promotion, how quickly could you confirm that a discount was running against inventory that existed?	Real-time inventory visibility means promotions run against live stock and discrepancies surface immediately, not after a customer complains.
If someone returned the same item twice across your online and in-store channels, would anything flag it or would both systems approve it independently?	A unified inventory layer flags duplicate returns across channels automatically before they're approved.
What's the fastest your BOPIS inventory reflects accurately across every channel after an in-store sale?	Updates happen in minutes, and every channel reflects the same reality in real time.

Reason for concern: If your team's answers rely on after-the-fact reconciliation, manual verification or cross-channel policies that sit outside the systems themselves, the seam is open.

How Dell Technologies helps you trust your inventory data

AI-ready Dell PCs powered by Intel® Core™ Ultra processors, combined with Dell NativeEdge orchestration, analyze transactions and inventory signals locally, ensuring real-time alignment and fraud prevention. Windows 11 Pro adds built-in security and device management so systems remain protected and consistent across locations.

Dell edge infrastructure, such as PowerEdge servers, can process operational data generated in stores, from POS systems and inventory scanners to cameras and shelf sensors. This allows real-time insights to be produced where the data originates.

Dell NativeEdge provides the orchestration layer that allows retailers to deploy, monitor and update these capabilities across stores from a centralized platform.

The result is a consistent view between ecommerce systems and store inventory. With systems aligned, retailers see fewer stockouts, more accurate fulfillment and stronger promotional planning, while opportunities for return fraud and promotion abuse shrink.

SECTION 02

The transaction seam

Are your transactions evaluated across the full omnichannel journey?

Cross-channel fraud doesn't look suspicious channel by channel. Each system evaluates its own transaction correctly: the POS sees a legitimate return, the ecommerce platform sees a valid order, the fraud tool scores the checkout as low risk.

When your systems evaluate transactions across channels together, the picture changes. You can see a customer's full journey, from the promo code and online order to in-store pick up and return, as a single thread rather than separate events.

That visibility helps catch fraud faster and gives you better insight into which promotions are working, which customers are your most valuable and where your policies are being stretched.

Cross-channel visibility is one of the clearest operational advantages available to retailers running omnichannel operations, and it's one of the most underutilized. It can't happen when systems are operating in parallel. They need to share data.

The benefits of closing the transaction seam

Cross-channel visibility reveals patterns individual systems miss:

- Detect suspicious activity as transactions occur across POS and ecommerce.
- Surface self-checkout anomalies in real time.
- Identify policy abuse across stores and digital channels.
- Connect returns, purchases and accounts into a single transaction view.
- Shift loss prevention from reactive investigation to continuous monitoring.

How Dell Technologies helps you spot patterns across transactions and channels

Dell Technologies closes the transaction seam by enabling systems to evaluate activity across channels together, using Dell PCs with local processing capabilities and Dell NativeEdge for centralized management.

Intel® Core™ Ultra processors with built-in NPU acceleration enable this data to be processed locally on the device, so there's no round trip to a central system and no latency window for fraud to exploit.

How strong is your transaction seam?

Ask your team	What a strong seam looks like
If the same customer account placed an online order, picked it up in-store and used a promo code within 48 hours, would you see all three transactions together anywhere, or would each system handle it separately?	All three events are visible in a single transaction view, and activity is connected across accounts, channels, and time.
When a customer returns something in-store that they bought online, do you have the original transaction details in front of you before you approve it or are you taking their word for it?	The original transaction is surfaced automatically at the point of return, regardless of which channel it came through.
If someone tested a stolen account with a small purchase at your online store and followed up with a larger one in-store two days later, at what point would you see that as a pattern?	Cross-channel activity is evaluated together in real time, so the pattern surfaces before the second transaction is approved.
How long between a suspicious transaction happening and you finding out about it, and does that differ depending on which channel it came through?	Detection happens at the same speed across all channels.

Reason for concern: For a small retailer, patterns may not surface until the losses have already started. The diagnostic isn't designed to determine whether fraud is happening. It's designed to reveal whether your architecture would tell you if it were.

The rise of return fraud and why it’s a two-seam problem

In 2025, returns value surged to $850 billion, while fraudulent returns tripled, rising from $25 million to $76.5 billion.[5] Although retailers might be tempted to tighten return policies, doing so could impact profits, as indicated by the 57% of shoppers who say they would stop shopping with a retailer that charged them for a return.[6]

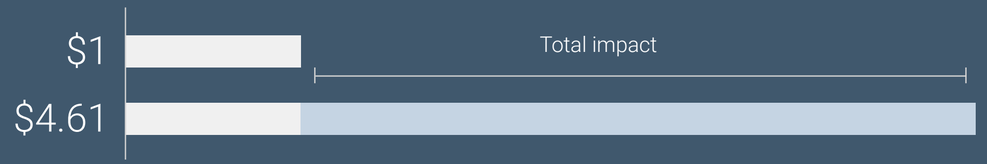
That's the trap and it persists because neither response addresses what's actually happening. A fraudulent return doesn't succeed because your policy is too generous. It succeeds because two systems that should be talking to each other aren't moving fast enough.

The transaction layer needs to recognize the original purchase before the return is approved. The inventory layer needs to register that return before the same item can be submitted again. When both seams are closed, that window doesn't exist. When either one is open, fraud moves faster than your systems do.

The retailer’s dilemma:

The solution isn't a stricter policy or a looser one. It's inventory and transaction data that moves as fast as your transactions do, so the decision gets made with complete information, before the return is approved.

For every $1 of ecommerce fraud, retailers lose $4.61 in total costs once chargebacks, operational overhead and lost customers are factored in.[7]



SECTION 03

The device seam

Do your legacy devices carry the same security posture as your new ones?

Most retail environments contain a mix of devices at different stages of their lifecycle. Some were configured when you opened. Others came online during a system refresh, a new location launch or when a register failed mid-shift and needed to be replaced the same day.

Each of those moments is a configuration event. When a new store opens, the goal is that it works exactly like every other store from the first transaction: same setup, same security policies, same IT standards. When a device gets replaced, the goal is the same. Without centralized device management, organizations depend on manual configuration done under pressure, and it creates device drift over time.

The longer that drift goes undetected, the larger the exposure.

Sixty-six percent of retail endpoints currently carry at least one high-risk vulnerability,[8] and research from Microsoft shows that 80–90% of successful ransomware attacks originate from unmanaged devices.[9]

The goal is knowing the moment any device in your fleet drifts from that standard. Centralized device management makes that possible, whether you're onboarding a new location, replacing a failed register or pushing a security update across every endpoint at once.

The benefits of closing the device seam

To exploit the device seam, an attacker just needs to find one endpoint that isn't properly managed. In a fleet that grew location by location, that endpoint is rarely hard to find.

To protect every endpoint in the retail environment, retailers need to:

- Establish hardware-based security controls.
- Maintain consistent security policies across the device fleet with centralized device management.
- Reduce exposure by discovering and managing any unmanaged endpoints.
- Enable faster device deployment across locations.

How Dell Technologies helps ensure security consistency

Dell Technologies zero-touch provisioning, powered by Windows 11 Pro and Intel vPro® platform, ensures consistent security configurations across all locations from day one, reducing vulnerabilities and IT overhead.

Centralized management tools let you monitor and maintain the entire device fleet from a single view, catch drift before it becomes a vulnerability, push updates without scheduling a site visit, and onboard a new location the same way every time.

The operational impact is measurable. Retailers using Dell Technologies commercial devices with Windows 11 Pro have reported up to 80% fewer helpdesk calls,[10] which in a small IT environment is the difference between a team that's firefighting and one that's supporting the business.

How consistent is your device posture?

Ask your team	What a strong seam looks like
When you opened your most recent location, how long between the first transaction processed and that store's endpoints being fully enrolled in centralized device management?	New locations come online already enrolled in centralized management with the same configuration as every other store, from day one.
Right now, do you know which devices across your locations are running a configuration that differs from your standard setup?	A centralized management view shows the full device fleet in real time, so technical drift is visible before it becomes a vulnerability.
If a phishing attempt targeted a staff member at your newest location today, would the outcome differ from the same attempt at your original store?	Security posture is consistent across locations because it's set at the device level and doesn't depend on individual behavior.
When did you last check for devices connected to your network that aren't inside your management framework?	The management platform continuously discovers unmanaged devices without requiring periodic audits.

Reason for concern: If any of these questions required you to estimate, check manually or ask someone at a specific location, your device fleet isn't being managed as a unified system. In a managed fleet, that uncertainty gets resolved before it becomes a vulnerability. In an unmanaged one, it often gets resolved after an incident.

What is device drift?

Device drift happens when endpoints that were originally configured the same way gradually diverge over time.

This can happen when:

- A register is replaced during a busy shift.
- A kiosk is installed during a promotion.
- A device misses a patch cycle.
- A new store launches with manual configuration.

Integrated systems unlock growth

Fraud doesn't create gaps in your systems; it finds them. Closing the gaps reduces risk and makes every part of your operation more reliable. Inventory you can trust. Transactions visible across every channel. And a device fleet that holds its standard from your first location to your latest.

Dell Technologies partners with retailers to build that unified foundation, so the systems you put in place today can scale with the business.

Learn more about retail solutions from Dell Technologies.

1. Deloitte, Retail Today, 2021.
2. Ibid.
3. Ibid.
4. MRC, 2024 Global eCommerce Payments & Fraud Report, 25th ed.
5. National Retail Foundation, 2025 Retail Returns Landscape, October 15, 2025.
6. Ibid.
7. LexisNexis True Cost of Fraud Study 2025.
8. Sophie Moreland, Retail Data Breach Statistics, 2026, Gitnux, February 13, 2026.
9. Microsoft Digital Defense Report 2023.
10. Commissioned study delivered by Forrester Consulting, “The Total Economic Impact™ of Windows 11 Pro Devices,” December 2022.

DELL Technologies