

i3 International SUCCESS STORY

*How a C-Store operator uncovered **\$33,500** in annualized risk at just **3 Locations** and **\$100,000** in cumulative loss— and turned it into a **45-store** rollout.
20 Cases. 85% Closed. 1 Per Week.*



In just 6 months and across a fraction of their footprint, AI-powered exception reporting revealed hidden loss patterns, systemic failures, and operational gaps that traditional surveillance never could — averaging approximately one new case every week.

THE CHALLENGE

Like many growing c-store operators, this multi-site convenience store and fuel retailer was dealing with loss and operational risk that traditional surveillance alone couldn't address. Isolated incidents were being handled reactively, but there was no systematic way to identify repeat transactional patterns, process weaknesses, or control gaps across locations.

The operator needed a solution that could surface not just what went wrong — but why it kept happening.

THE APPROACH

Working closely with i3 International's asset protection team, the operator deployed i3Ai Smart-ER — i3's AI-powered exception-based reporting solution — integrated with video surveillance through i3's Cloud Managed Services (CMS) across multiple locations. Rather than simply generating alerts, i3's team took a hands-on, investigative approach: reviewing transactional data, building cases, and presenting findings in weekly working sessions with the operator's leadership.

Over the course of roughly six months, this collaborative model produced 20 documented cases across three store locations — averaging approximately one new case per week — with 17 cases closed and three still in progress.



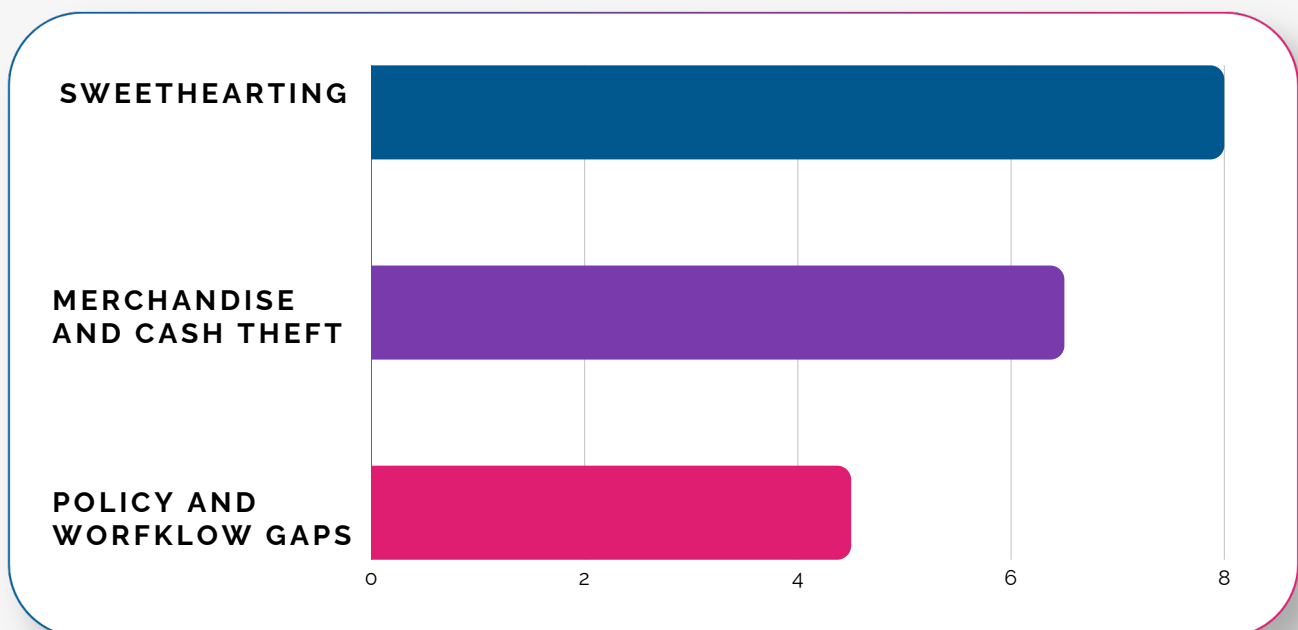
WHAT THE DATA REVEALED

i3Ai Smart-ER surfaced a diverse range of risk patterns, each pointing to a different area of operational exposure:

Sweethearting (8 cases): The most common finding, typically involving repeated patterns of items being voided, transactions being manipulated, or product leaving the store without proper payment. Several were ultimately classified as operational issues — still valuable because they highlighted where process controls were weak or inconsistently enforced.

Merchandise and cash theft (7 cases): Including scenarios involving change manipulation, transaction sequencing anomalies.

Policy and workflow gaps (5 cases): Employees ringing their own transactions, refund abuse, lottery handling irregularities, and discount overrides — each pointing to high-risk workflows where small controls could dramatically reduce exposure.



Based on the patterns identified across these 20 cases, the annualized risk exposure reached \$33,500 — approximately \$11,167 per store, per year. And that figure only reflects what was surfaced through transaction-level exception analysis, not total loss across all categories.

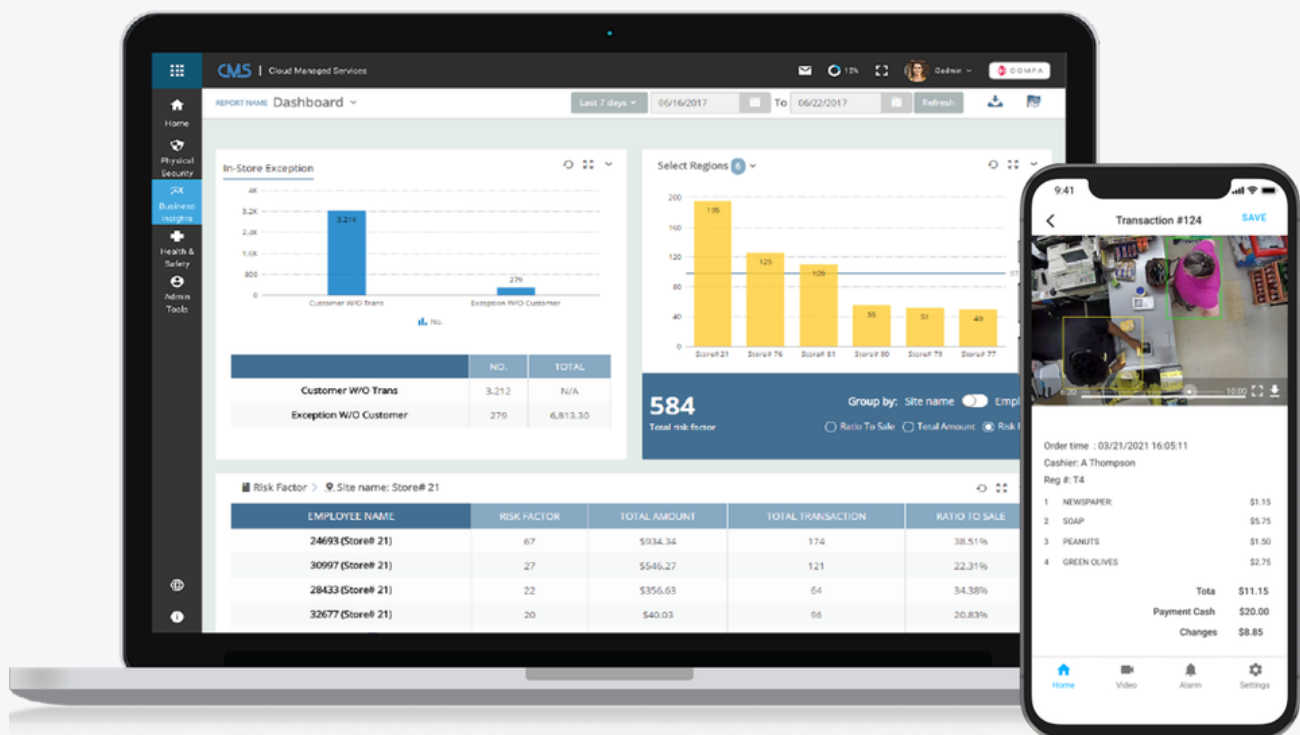
With just 3 locations covered over roughly 6 months and the majority of the operator's footprint still to be onboarded, the results were compelling enough that the operator committed to a 45-location rollout.

CASE SPOTLIGHT: A DECADE OF UNDETECTED CASH THEFT — STOPPED IN WEEKS

One case in particular illustrates both the speed and depth of i3's investigative approach.

A newly onboarded location — part of a second wave of stores added after the initial pilot — had no prior historical visibility when it was connected to i3Ai Smart-ER and CMS. Despite the lack of baseline data, the system surfaced high-risk activity almost immediately after transaction data became available.

Using exception-based reporting paired with video validation, i3's team uncovered a consistent and deliberate method of cash theft.



The employee would complete transactions, accept full cash payment from customers, and then void items post-tender while still providing change based on the original total. This created unrecorded excess cash in the register that was not tied to any sale. In other instances, items presented by customers were never scanned at all. The employee used the “No Sale” function to open the register and provide change, bypassing the POS system entirely.

What clearly established intent was the structured, repeatable nature of the behaviour. The employee was consistently observed manually tracking unrecorded cash on receipt paper, segregating those funds within the register, and removing the accumulated cash at the end of each shift. Handwritten notes were destroyed after each shift to conceal the activity.

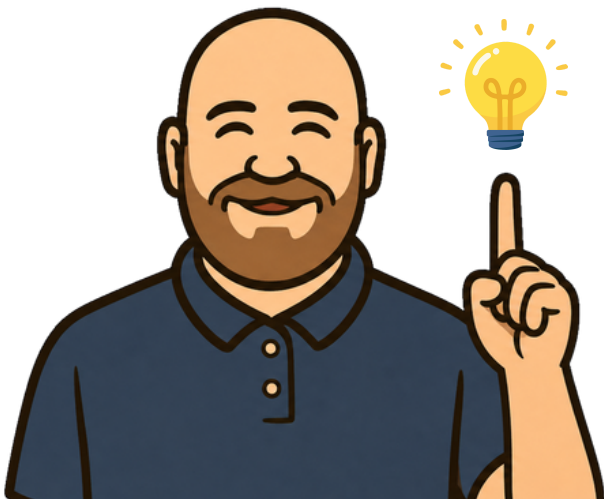
Following presentation of the findings, the employee admitted to the activity and confirmed it had been ongoing for approximately ten years – entirely undetected prior to implementation.

Based on data analytics and transaction pattern analysis, losses were conservatively estimated at approximately \$100 per shift. At an average of two shifts per week, this equates to roughly \$10,000 in annual losses. The employee later admitted to engaging in the activity for approximately ten years, which aligned with the findings identified through the analysis. Based on that admission and the conservative loss estimate, the cumulative impact is estimated to exceed \$100,000 in losses that went undetected and unaddressed over that period.

The employee was terminated, and the matter was escalated to law enforcement.

COMMENTARY FROM i3'S AP ANALYST

This single case demonstrates a critical point: exception reporting doesn't just find what's happening now. It finds what's been happening for years – and in a newly connected store with no historical data, it did so within weeks.



While individual cases can vary in scale, the value of the program is driven by the consistent identification of repeat behaviours – not reliance on isolated high-impact incidents.

BEYOND THE NUMBERS: OPERATIONAL DISCOVERIES THAT CHANGED THE BUSINESS

What set this engagement apart was not just the cases themselves, but the operational and technical issues that the investigative process uncovered along the way.

Payment system failures no one knew about

Through case review, i3's team identified a critical integration issue between the operator's payment terminals and POS system. In multiple instances, the payment terminal displayed a successful transaction while the POS did not register the payment. This meant merchandise was leaving the store unpaid for — not because of theft, but because of a system failure.

At the operator's request, i3 worked directly with both the POS provider and the payment processor, supplying concrete transaction examples that helped isolate and validate the issue. Without exception reporting paired with video, this systemic problem could have gone undetected indefinitely.

A workaround that created real risk

The investigation uncovered a recurring practice where staff were ringing car wash transactions at \$0.01 to generate customer codes — a workaround driven by a system limitation rather than intent. While not malicious, this practice obscured true sales data, weakened reporting accuracy, and created a pattern indistinguishable from intentional manipulation.

The operator acknowledged the issue and began working toward a proper POS-supported workflow to eliminate manual workarounds.

Camera placement and integrator alignment

During case development, i3 identified gaps in camera coverage that limited investigative effectiveness at certain locations. This led to a broader conversation about alignment between the operator, their integrator, and i3 — ultimately contributing to the operator's decision to transition to a new integrator, creating an opportunity to standardize placement guidelines and improve future installations.

A PARTNERSHIP, NOT JUST A PLATFORM

Throughout the engagement, i3 and the operator maintained weekly working sessions where cases were reviewed and presented in real time. This cadence kept momentum high, provided context behind findings, and ensured alignment on next steps.

The operator centralized all case intake through a single point of contact — a model that worked well during the early phase and is expected to evolve as additional stores are onboarded and case volume grows.

One area both teams identified for improvement was formalizing outcome reporting and case closure timelines, ensuring that investigative results are captured efficiently and fed back into reporting and detection logic for continuous improvement.

The investigations presented to the operator extended beyond identifying individual incidents and provided valuable insight into broader operational vulnerabilities. Through the review of case findings, transaction patterns, and observed behaviours, leadership was able to evaluate the effectiveness of existing policies, procedures, and internal controls. As a result, the organization implemented several meaningful changes aimed at strengthening oversight, increasing accountability, and reducing opportunities for fraud and operational losses. These improvements included enhancements to store-level controls, policy revisions, and increased management focus on high-risk activities. The outcome was a more proactive approach to risk management that helped minimize the company's overall exposure and improve operational integrity across the business.



FROM 3 STORES TO 45

Based on the strength of the initial engagement, the operator committed to rolling out i3Ai Smart-ER and CMS across 45 locations — a decision driven not just by the cases themselves, but by the depth of operational insight the program delivered.

As the rollout progresses, so does the value of i3's exception reporting capabilities. The engagement has already demonstrated how ad hoc exception development — building custom reports in response to emerging behaviours and system gaps — can stay ahead of risk patterns before they become entrenched.

Issues like credential sharing, suspended transactions used for informal employee purchases, penny-based car wash workarounds, and payment system failures were all surfaced precisely because i3's team had the flexibility to explore data outside of rigid report definitions.

As more stores come online, i3Ai Smart-ER will enable better segmentation by store, role, time of day, and transaction context — reducing noise, improving signal quality, and ensuring that exception reporting remains actionable rather than overwhelming as the operation scales.

KEY RESULTS AT A GLANCE

While the scale of individual cases can vary, the underlying patterns identified in this engagement are not unique to this operator.

Across convenience and fuel retail environments, we consistently observe similar behaviours — including transaction void misuse, refund manipulation, and cash handling gaps — driven by common operational workflows and control limitations.

These behaviours are typically not isolated incidents, but repeatable patterns tied to how POS systems are used in day-to-day operations.

In most environments, meaningful behavioural patterns begin to surface within the first few weeks of analyzing transaction data, even without historical baselines.

WHY IT MATTERS

This engagement demonstrates that the real value of exception-based reporting isn't just catching theft — it's building a smarter, more resilient operation. By combining i3Ai Smart-ER's AI-powered transaction analysis with video verification and hands-on investigative expertise, this c-store operator:

Gained visibility into risks they didn't know they had

Fixed systemic issues that were silently costing them money

Built confidence in the program to expand from a 3-store pilot to a 45-location enterprise rollout

Most operators see a steady cadence of actionable cases tied to both employee behaviour and operational gaps, with value increasing as more locations and data are incorporated.

Ready to uncover what's hiding in your transaction data? Schedule a call with i3 International today to learn how i3Ai Smart-ER and Cloud Managed Services can help your organization identify hidden risk and drive operational improvement



<https://www.i3international.com/>



<support.i3international.com/contact-us/request-demo>

