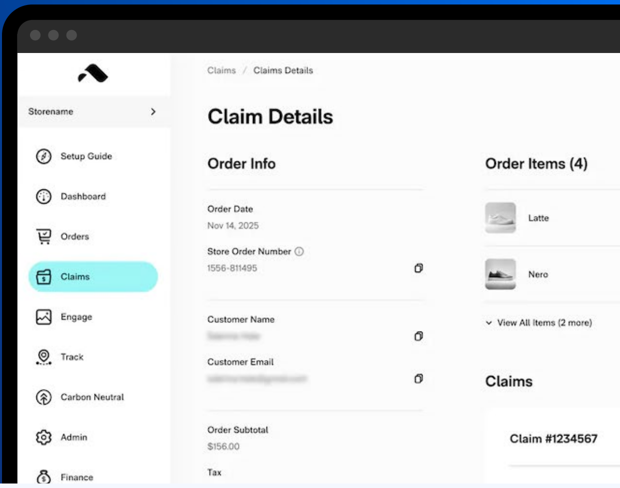
SHIELD | ROUTE

Case Study

Route Partners SHIELD to Reduce Fake Claim Financial Exposure by 99% and Accelerate Refund Processing



Claim Details

Order Info

Order Date
Nov 14, 2025

Store Order Number
1556-811495

Customer Name
[redacted]

Customer Email
[redacted]

Order Subtotal
$156.00

Tax

Order Items (4)

Latte

Nero

View All Items (2 more)

Claims

Claim #1234567

> “Fraud poses a significant risk to our merchant partners. We needed a solution that could extend our product capabilities to proactively prevent it. SHIELD’s AI-powered device intelligence platform has allowed us to better identify and block fraudulent claims, improve operational efficiency, and preserve customer trust. It’s now a core component of our long-term fraud prevention strategy.”

Christian Hartman
Senior Product Manager, Route

Key Takeaways

50% boost in claims denied for fraudulent activity

200% increase in the ability to flag the same customer acting as different users

99% reduction in fraudulent claim payouts linked to coordinated multi-account abuse

Business Challenge: Refund Fraud

In today’s fast-paced e-commerce landscape, customer experience doesn’t end at checkout. It extends to tracking, delivery, and post-purchase support. Route is redefining how consumers interact with their online orders. However, refund fraud is surging, with fraudsters exploiting post-purchase policies in increasingly sophisticated ways.

Companies like Route face a growing wave of fraudulent refund claims. Common fraud tactics include filing multiple claims across different accounts and abusing issue resolution processes for lost or damaged items.

Existing methods of refund fraud prevention, primarily email-based verification, fail to address the scale and complexity of these attacks.

Customer Profile

Route is the leader in post-purchase experience, empowering brands and their customers with shipping insurance, real-time tracking, and fast issue resolution. Trusted by 13,000+ leading brands, Route has transformed potential delivery issues into opportunities for customer loyalty and long-term brand success.

Industry

E-commerce Tech

Region

Global

Fraudsters easily bypass these measures with stolen identities, often masking their activity with bots, emulators, VPNs, and proxies.

The impact of refund fraud is twofold, hurting both revenue and customer experience:

- Revenue loss from false positives and incorrect approvals.
- Damaged brand trust when legitimate customers are flagged as fraudulent.

The Solution: Powered by SHIELD AI, Route Keeps Refund Fraud in Check

Route turned to SHIELD's device-first fraud intelligence platform to combat these challenges. SHIELD's Device ID provides Route with a persistent and accurate identifier that links fraudulent activity across sessions and accounts, enabling Route to identify multiple refund claims originating from the same fraudulent device, even if they appear completely unrelated.

SHIELD's fraud intelligence goes beyond surface-level detection to expose the tools & tactics fraudsters rely on. Whether they are using auto-clickers to mass-submit refund requests, emulators to mimic legitimate devices, or VPNs to hide their true location, SHIELD returns this intelligence in real time, empowering Route to take instant action.

With real-time fraud detection, Route can block fraudulent claims before they escalate, eliminating the need for costly damage control. Since SHIELD operates without requiring Personally Identifiable Information (PII), Route stays compliant with global data privacy laws while keeping its platform secure.

The Road Ahead

Since deploying SHIELD, Route has strengthened its refund claim processes:

- **200% increase in the ability to flag the same customer acting as different users**
  With SHIELD Device ID and Device Intelligence, Route can now accurately detect when a single fraudster is operating multiple accounts to submit repeat claims. This sharp increase in visibility has made it significantly harder for fraudsters to hide behind fake identities and abuse the system.

- **99% reduction in fraudulent claim payouts linked to coordinated multi-account abuse:**
  SHIELD's real-time fraud intelligence empowers Route to proactively block suspicious claims linked to device manipulation or spoofing. As a result, payments to fraudulent actors posing as different customers have been eliminated, protecting Route's bottom line while preserving claim integrity.

- **50% boost in claims denied for fraudulent activity:**
  By identifying fraud patterns and malicious tools like emulators, VPNs, and auto-clickers, Route has been able to confidently deny more fraudulent claims without affecting genuine customers. This increase reflects stronger fraud defenses and improved accuracy in identifying real customers.

A Future of Seamless and Secure Shopping

By integrating SHIELD's device-first fraud intelligence, Route has taken its fraud prevention strategy to the next level, ensuring fast, secure, and seamless post-purchase protection for businesses and customers alike.