tailed *report*

The Silent Multi-Billion Dollar Threat Attacking eCommerce

Fake Tracking ID (FTID) Fraud Industry Report

September 2024

www.tailed.ai contact@tailed.ai

Contents

Introduction

Fake Tracking ID (FTID) Fraud has rapidly grown to become the largest and most expensive return fraud plaguing eCommerce.

In September 2023, The U.S. Attorney's Office indicted a Michigan man for his role in a $4 million refund fraud operation. It was the first-ever U.S. arrest for a little-known but highly sophisticated form of fraud and drew little notice. Just six months later, the issue gained national attention when CNBC reported “Refund Fraud Schemes Promoted on Telegram are Costing Amazon and Other Retailers Billions.” For many, this was their first time hearing about the sophisticated scheme known as Fake Tracking ID (FTID) fraud.

FTID fraud has stayed under the radar for so long because it is designed to be invisible, allowing individuals to steal millions without detection. First becoming mainstream during the COVID-19 pandemic, it has grown into **a multi-billion dollar problem** for retailers and the preferred method of fraud for sophisticated cyber criminals commercializing refund fraud.

FTID fraud is carried out by loosely organized crime rings that offer "refund-fraud-as-a-service." This enables thousands of **individuals with no prior fraud experience to partner with seasoned cybercriminals** to receive refunds. Once fraudsters identify a vulnerability in a brand, they quickly spread the information through a network of over 100,000 anonymous criminals on platforms like Telegram, leading to potentially millions in losses in a matter of weeks.

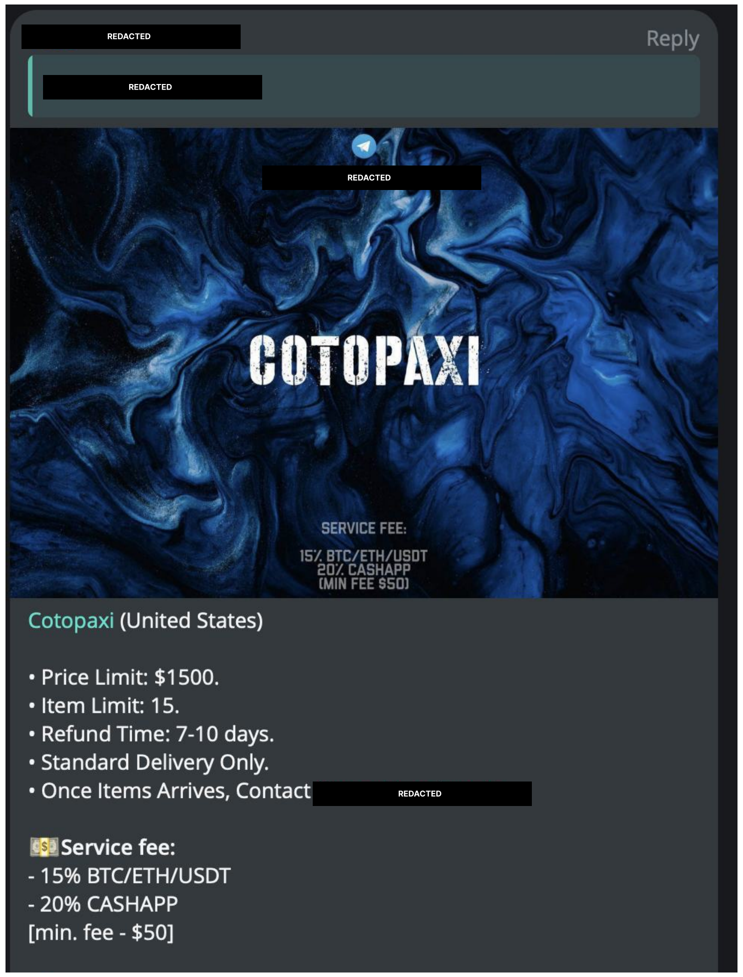
The primary targets of this fraud are rising direct-to-consumer (D2C) brands, many of which lack the resources to detect and combat such sophisticated schemes. This report aims to help retailers understand how FTID fraud works, why it’s so difficult to detect, and **what steps they can take to protect their businesses from this growing eCommerce threat.**

Telegram: The Fraudster's Platform of Choice

Overview

Founded in 2013 by Pavel Durov, Telegram is an encrypted messaging platform designed for secure and private communication. Durov's strong stance on data security and free speech has led him to resist cooperation with U.S. and international regulators. While this protects user privacy, it also places Telegram beyond the reach of authorities, making it an ideal platform for illicit activities.

Previously, refund fraud was primarily confined to the dark web, a hidden part of the internet accessible only through specialized software. The dark web's complexity, anonymity, and inherent risks of hackers and malicious actors kept FTID as an underground form of fraud, inaccessible and unknown to the ordinary person. The rise of Telegram pushed FTID out to the masses and created a massive organized refunding underworld.



Cotopaxi (United States)

• Price Limit: $1500.
• Item Limit: 15.
• Refund Time: 7-10 days.
• Standard Delivery Only.
• Once Items Arrives, Contact REDACTED

💵**Service fee:**
- 15% BTC/ETH/USDT
- 20% CASHAPP
[min. fee - $50]

Figure 1: *A Telegram channel specializing in refund fraud advertises specific retailers that are vulnerable to fraud. The store name, upper limit on return value, and refund timeline are shown.*

Commercialization of Refund Fraud

Background

Refund fraud has existed for decades but has surged with the growth of eCommerce. What began as isolated incidents has now evolved into a large-scale operation, driven by organized crime rings offering "Refund-Fraud-as-a-Service" (RFaaS).

The National Retail Federation estimates that $101 billion in merchandise was fraudulently returned in the U.S. last year, with $13.70 of every $100 in returns being fraud—more than double the rate in 2020 when return fraud accounted for just 5.9% of returns.

Fake Tracking ID (FTID) Fraud

The most rapidly growing method of fraud in RFaaS, involving the manipulation of shipping labels to make it appear that a return package was delivered. This false positive return triggers automatic refunds or can be used as evidence to social engineer customer service. Criminals have turned this fraud into a full-time operation.

Unlike older fraud methods, like Chargeback and Item-Not-Received (INR) Fraud, FTID doesn't rely on exploiting delivery errors or financial institutions; instead, it manipulates the retailer's own return processes, making it much harder to detect and prevent.

To understand the rise of FTID fraud, it is important to learn about Telegram, an encrypted messaging platform that has grown in parallel to FTID and enabled the rise of 40,000+ member refunding rings.

Tailed’s return audits find that at minimum 5% of all returns are connected to FTID fraud.

tailed *statistic*

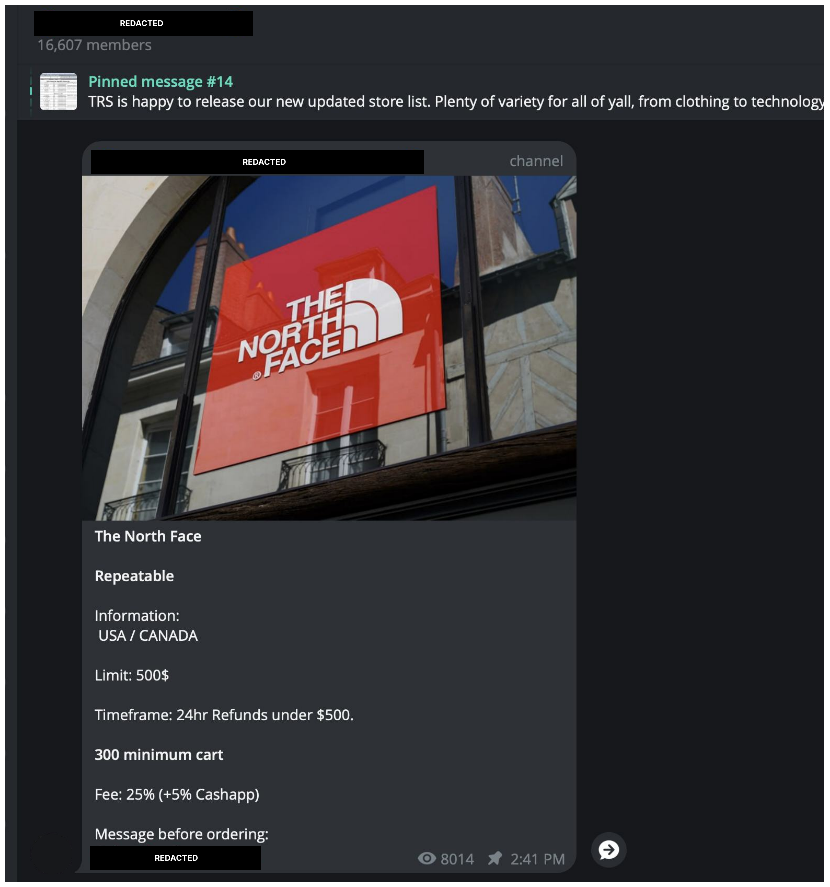
The Anatomy of the Refunding Underworld

Background

Refunding began as a simple scam but has since evolved into **a highly structured industry**. It now operates as an ecosystem of refund-fraud-as-a-service providers that work together to execute FTID fraud, with **some fraud channels on Telegram amassing over 40,000 members**. These channels can be divided into three primary categories, listed below.

Refunding Services

Refunding services offer **a complete solution for individuals seeking fraudulent refunds.** Typically, customers submit requests via Google Forms, providing details like login information for the brand they wish to defraud. The service then handles everything — from shipping out manipulated return labels to social engineering customer service reps. Once the refund has been granted, the service charges a fee, typically between 10% and 25% of the refund amount.



REDACTED
16,607 members

Pinned message #14
TRS is happy to release our new updated store list. Plenty of variety for all of yall, from clothing to technology

REDACTED channel

The North Face

Repeatable

Information:
USA / CANADA

Limit: 500$

Timeframe: 24hr Refunds under $500.

300 minimum cart

Fee: 25% (+5% Cashapp)

Message before ordering:
REDACTED

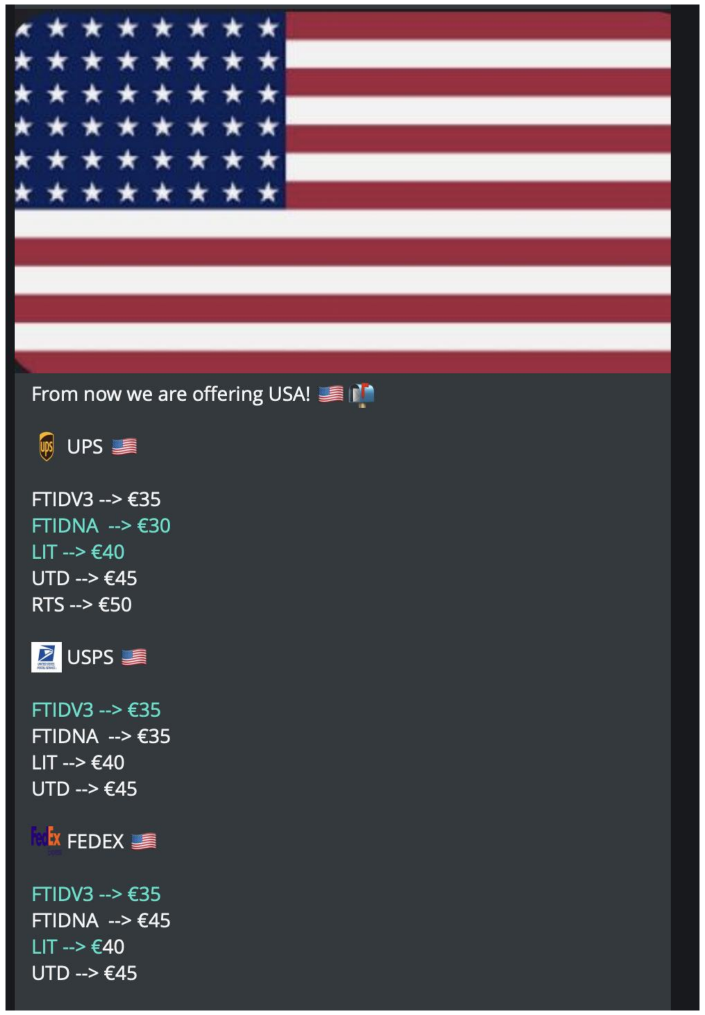
8014 2:41 PM

Figure 2: *A refunding service with 16,000+ members advertises a brand they will be able to refund for their customers within 24 hours for a 25% fee.*

Boxing Services

Boxing services manipulate return shipping labels to divert returns from their intended destination. This allows refunding services or more experienced fraudsters to outsource this technical task while managing the rest of the process.

The prices range from $20-$50 per edited label.



From now we are offering USA! 🇺🇸 📬

UPS 🇺🇸

FTIDV3 --> €35
FTIDNA --> €30
LIT --> €40
UTD --> €45
RTS --> €50

USPS 🇺🇸

FTIDV3 --> €35
FTIDNA --> €35
LIT --> €40
UTD --> €45

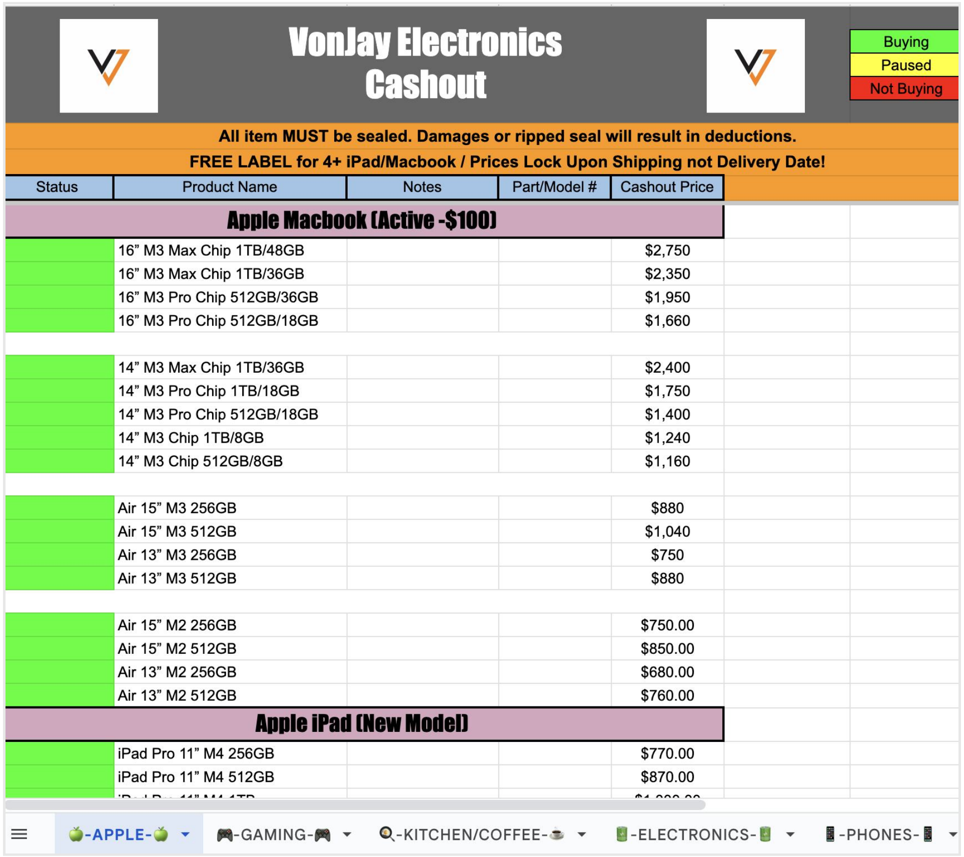
FEDEX 🇺🇸

FTIDV3 --> €35
FTIDNA --> €45
LIT --> €40
UTD --> €45

Figure 3: *A Boxing Service on Telegram advertising their services. Here, they advertise that the label manipulation process is on discount.*

Cashout Groups

Cashout groups operate as legal entities and buy up merchandise in bulk for below-retail prices. Unfortunately, many of the items they purchase are obtained through fraudulent means. These groups then resell the products at discounted prices on platforms like Amazon, drawing from the original brand's sales. This practice not only damages brands by encouraging demand for fraudulently sourced goods but also undermines their marketing efforts, pricing strategies, and overall brand integrity.



VonJay Electronics
Cashout

🟩 Buying
🟨 Paused
🟥 Not Buying

All item MUST be sealed. Damages or ripped seal will result in deductions.
FREE LABEL for 4+ iPad/Macbook / Prices Lock Upon Shipping not Delivery Date!

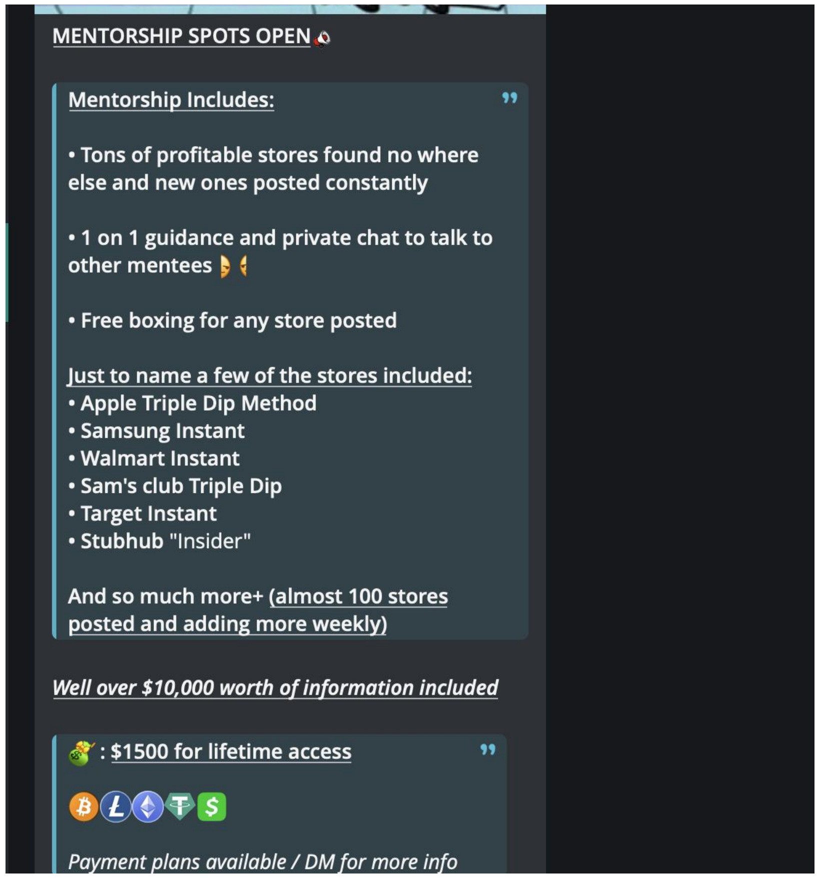
Status	Product Name	Notes	Part/Model #	Cashout Price
Apple Macbook (Active -$100)				
🟩	16" M3 Max Chip 1TB/48GB			$2,750
🟩	16" M3 Max Chip 1TB/36GB			$2,350
🟩	16" M3 Pro Chip 512GB/36GB			$1,950
🟩	16" M3 Pro Chip 512GB/18GB			$1,660
🟩	14" M3 Max Chip 1TB/36GB			$2,400
🟩	14" M3 Pro Chip 1TB/18GB			$1,750
🟩	14" M3 Pro Chip 512GB/18GB			$1,400
🟩	14" M3 Chip 1TB/8GB			$1,240
🟩	14" M3 Chip 512GB/8GB			$1,160
🟩	Air 15" M3 256GB			$880
🟩	Air 15" M3 512GB			$1,040
🟩	Air 13" M3 256GB			$750
🟩	Air 13" M3 512GB			$880
🟩	Air 15" M2 256GB			$750.00
🟩	Air 15" M2 512GB			$850.00
🟩	Air 13" M2 256GB			$680.00
🟩	Air 13" M2 512GB			$760.00
Apple iPad (New Model)				
🟩	iPad Pro 11" M4 256GB			$770.00
🟩	iPad Pro 11" M4 512GB			$870.00

Figure 4: *A Cashout Group listing fraudulent items for resale.*

Fraud Mentorships

Fraud mentorships are exclusive groups that teach individuals techniques for manipulating return shipping labels, social engineering customer service, and maintaining operational security (OPSEC) to avoid detection.

Entry fees typically range from $1,000 to $5,000.



MENTORSHIP SPOTS OPEN 📢

Mentorship Includes:

- Tons of profitable stores found no where else and new ones posted constantly
- 1 on 1 guidance and private chat to talk to other mentees
- Free boxing for any store posted

Just to name a few of the stores included:
- Apple Triple Dip Method
- Samsung Instant
- Walmart Instant
- Sam's club Triple Dip
- Target Instant
- Stubhub "Insider"

And so much more+ (almost 100 stores posted and adding more weekly)

Well over $10,000 worth of information included

💰: $1500 for lifetime access

Payment plans available / DM for more info

Figure 5: *An advertisement for a fraud mentorship posted in a refunding forum. The poster advertises that the mentorship provides access to brand employee "insiders" and exclusive fraud methods.*

The Financial Impact of FTID Fraud

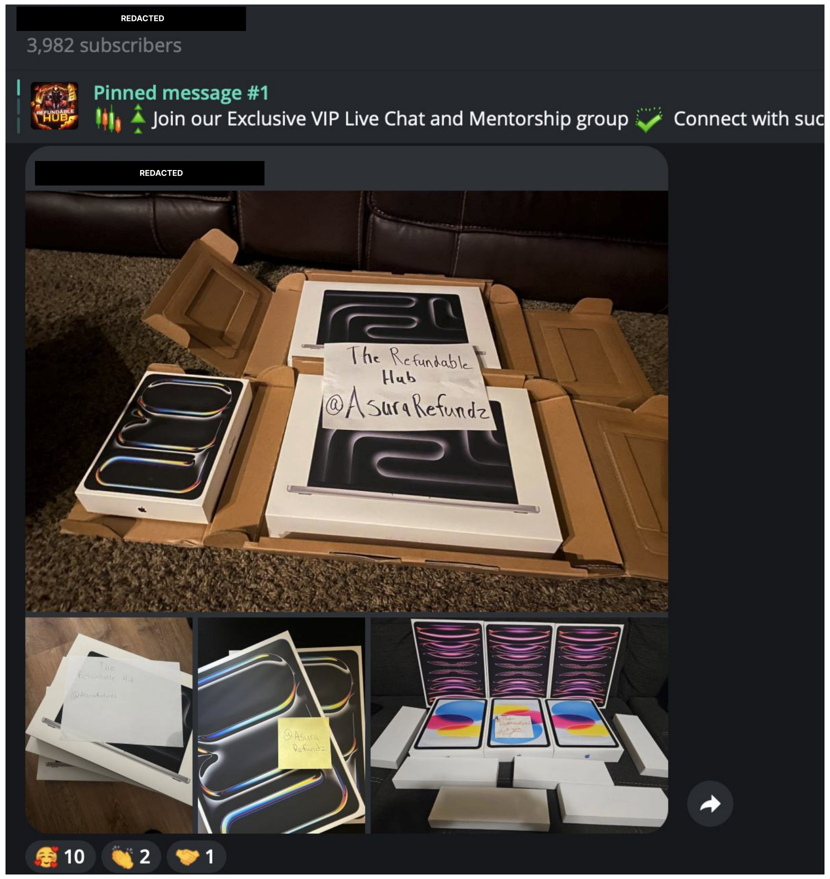
Positive Feedback Loops

In order to target brands for their customers, fraud services conduct surveillance by placing small test orders to assess refund policies or susceptibility to social engineering. Once a retailer is deemed easy to exploit, a damaging feedback loop is triggered.

Refund-fraud-as-a-service is a highly competitive industry. These services regularly post "vouches"—evidence of successful fraud against retailers—to demonstrate their effectiveness and attract new customers. This practice rapidly spreads information about the retailer's vulnerabilities.

If a refunding group with 20,000 members posts successful fraud, and just 10%—2,000 members—target the same company for $1,000 each, the loss would be **$2 million**.

tailed *statistic*



REDACTED

3,982 subscribers

Pinned message #1

Join our Exclusive VIP Live Chat and Mentorship group ✅ Connect with suc

REDACTED

Figure 6: *A refunding service posts vouches of successfully refunded Apple products. Notes with the service name are placed on the refunded items to prove the refund was gained through them.*

The above scenario is conservative, as it assumes the information is only shared with one fraud group and the average fraudster takes $1,000 from the brand.

Network Effect

In reality, details about vulnerable retailers spread quickly across multiple refunding channels on platforms like Telegram. Also, many fraudsters operate on a larger scale, treating refund fraud as a full-time business and defrauding brands for tens of thousands of dollars. For example, The Wall Street Journal reported a case in which PacSun faced losses of over $24,000 due to a single customer fraudulently returning 250 orders.

Certain cashout groups monitor fraud trends and, upon identifying a heavily defrauded brand, will offer to buy the products at a discount, giving fraudsters another reason to target the brand.

> When interviewed, a Senior Fraud Analyst in the cookware industry confirmed that their losses to FTID fraud were **“well above $10 million.”**

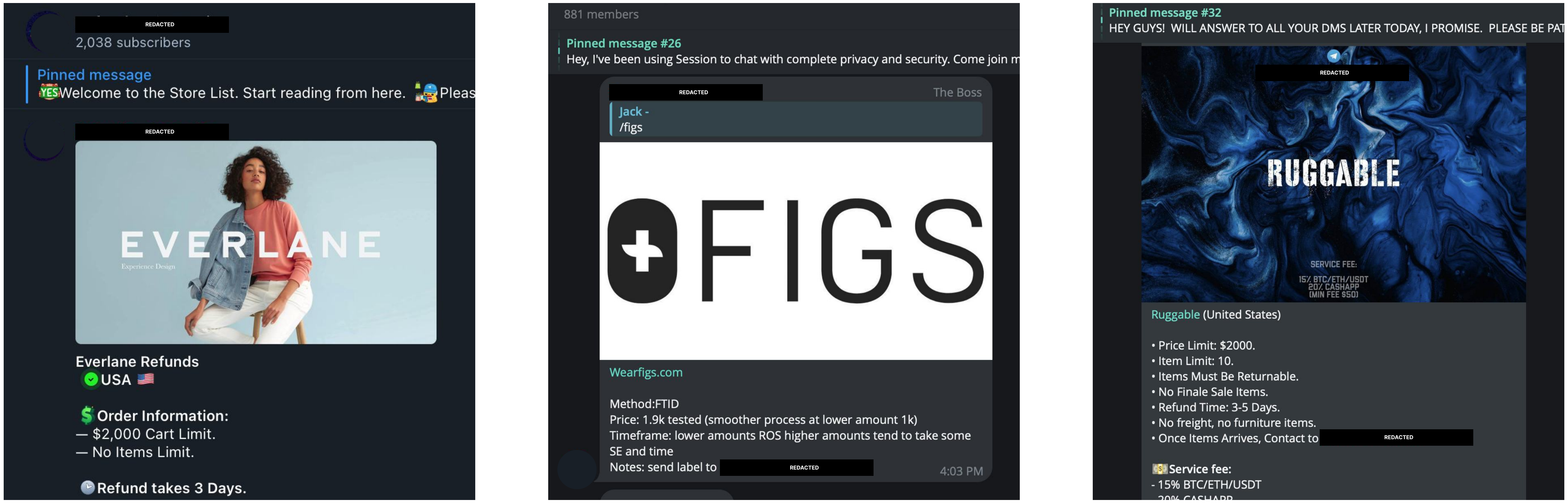
Breaking Down FTID Fraud: A Step-by-Step Guide

Overview

FTID fraud is a multi-step process that enables fraudsters to receive refunds while actually keeping the merchandise. Here is how it works using a “boxing service:”

1) Store Advertisement

An individual fraudster learns about a new exploitable brand in a refund-fraud-as-a-service group. These groups advertise exploitable stores to attract fraudsters, who pay the RFaaS group to defraud the companies on their behalf.



REDACTED
2,038 subscribers

Pinned message
YES Welcome to the Store List. Start reading from here. Pleas

REDACTED

Everlane Refunds
✓ USA

$ Order Information:
— $2,000 Cart Limit.
— No Items Limit.

Refund takes 3 Days.

881 members

Pinned message #26
Hey, I've been using Session to chat with complete privacy and security. Come join m

REDACTED The Boss
Jack -
/figs

Wearfigs.com

Method:FTID
Price: 1.9k tested (smoother process at lower amount 1k)
Timeframe: lower amounts ROS higher amounts tend to take some SE and time
Notes: send label to REDACTED 4:03 PM

Pinned message #32
HEY GUYS! WILL ANSWER TO ALL YOUR DMS LATER TODAY, I PROMISE. PLEASE BE PAT

REDACTED

Ruggable (United States)

- Price Limit: $2000.
- Item Limit: 10.
- Items Must Be Returnable.
- No Finale Sale Items.
- Refund Time: 3-5 Days.
- No freight, no furniture items.
- Once Items Arrives, Contact to REDACTED

Service fee:
- 15% BTC/ETH/USDT
- 20% CASHAPP

Figure 7a-7c: *Telegram channels advertising specific retailers vulnerable to fraud. The store name, upper limit on return value, and refund timeline are shown.*

2) Return Created

The fraudster places an online order with the target brand. Once the merchandise is received, the fraudster requests a return label and then sends the label to the refund-fraud-as-a-service provider.

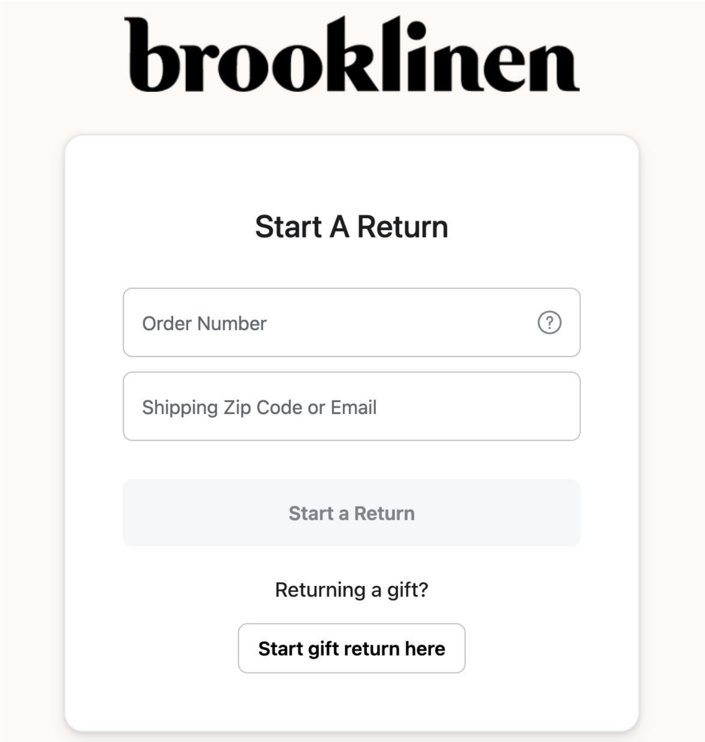
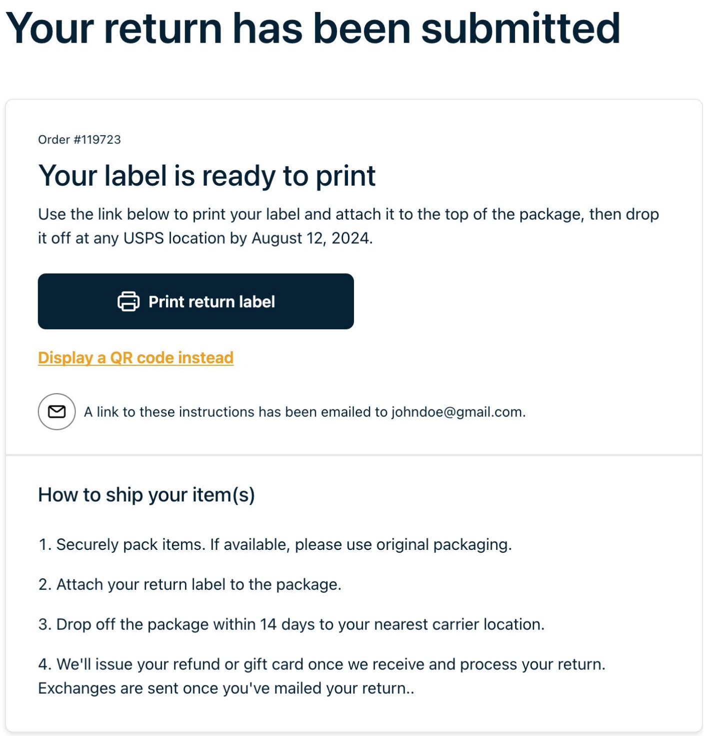


Figure 8a: *Return started on Returns portal*


Your return has been submitted

Order #119723

Your label is ready to print

Use the link below to print your label and attach it to the top of the package, then drop it off at any USPS location by August 12, 2024.

A link to these instructions has been emailed to johndoe@gmail.com.

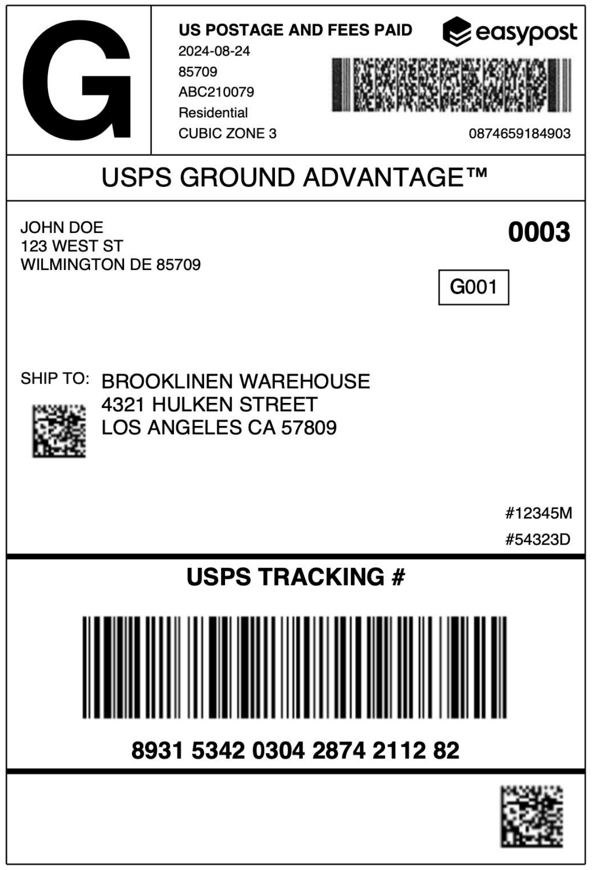
How to ship your item(s)

1. Securely pack items. If available, please use original packaging.
2. Attach your return label to the package.
3. Drop off the package within 14 days to your nearest carrier location.
4. We'll issue your refund or gift card once we receive and process your return. Exchanges are sent once you've mailed your return..

Figure 8b: *Return submitted, label generated*

3) Label Edit

The refund fraud-as-a-service provider systematically alters the barcode and/or QR code of the return label on the fraudster's behalf. Specifically, they change the shipment's destination address in the barcode metadata as well as on the label itself to a random address near—but not at—the original delivery address.



G

US POSTAGE AND FEES PAID
2024-08-24
85709
ABC210079
Residential
CUBIC ZONE 3

easypost

0874659184903

USPS GROUND ADVANTAGE™

JOHN DOE
123 WEST ST
WILMINGTON DE 85709

0003

G001

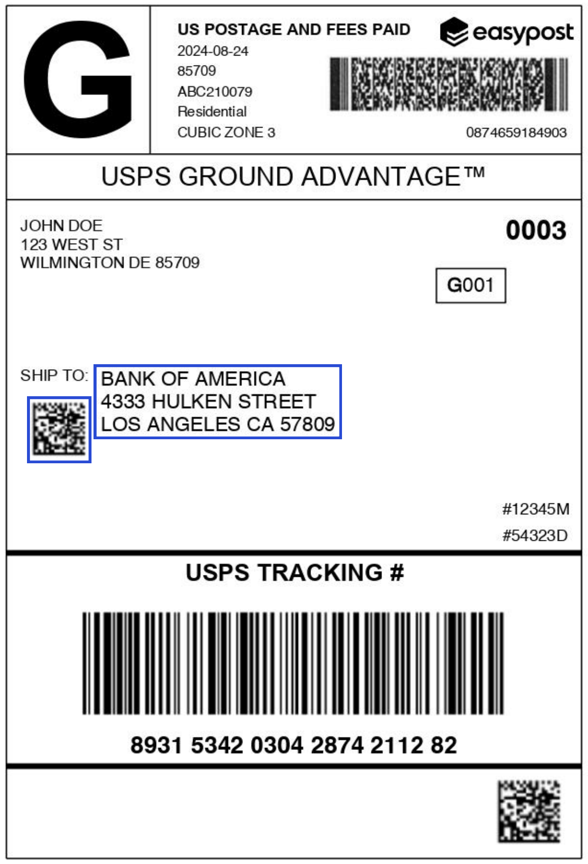
SHIP TO: BROOKLINEN WAREHOUSE
4321 HULKEN STREET
LOS ANGELES CA 57809

#12345M
#54323D

USPS TRACKING #

8931 5342 0304 2874 2112 82

***Figure 9a:** Original label before edit. Intended destination is Brooklinen's Return Warehouse.*



G

US POSTAGE AND FEES PAID
2024-08-24
85709
ABC210079
Residential
CUBIC ZONE 3

easypost

0874659184903

USPS GROUND ADVANTAGE™

JOHN DOE
123 WEST ST
WILMINGTON DE 85709

0003

G001

SHIP TO: BANK OF AMERICA
4333 HULKEN STREET
LOS ANGELES CA 57809

#12345M
#54323D

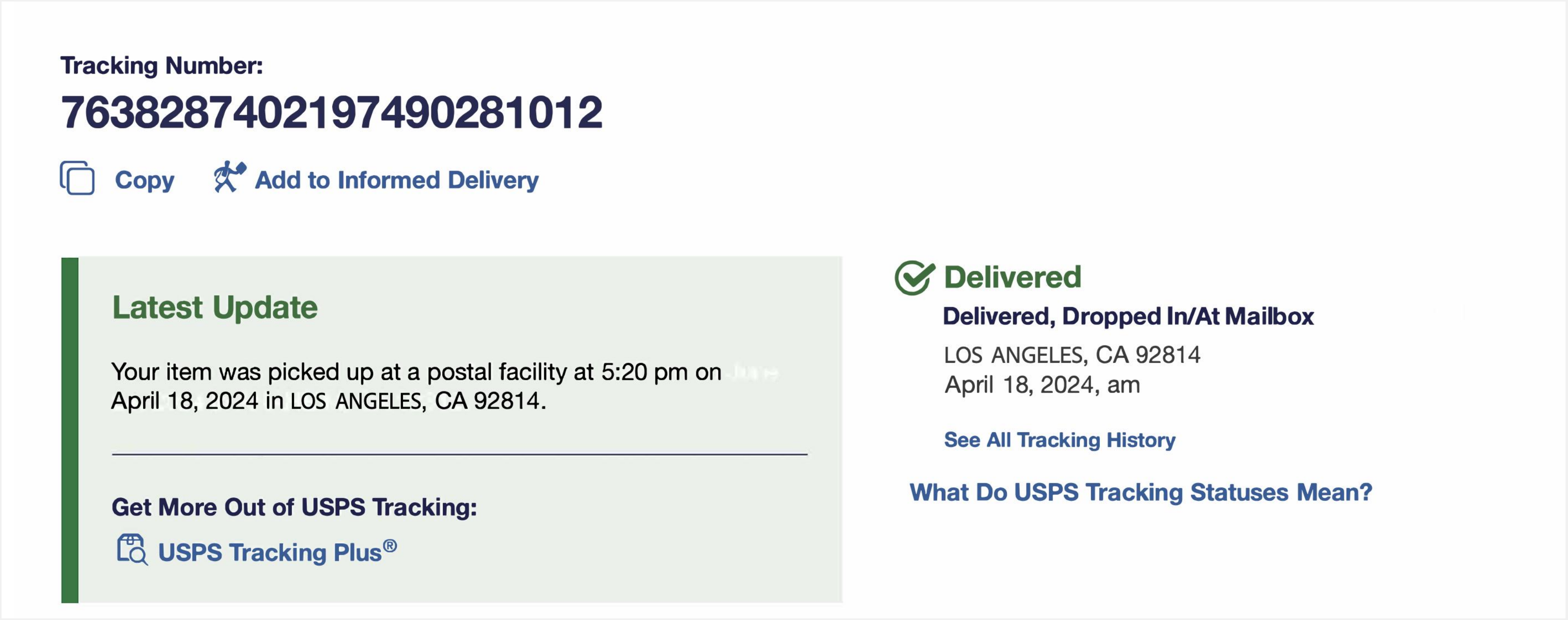
USPS TRACKING #

8931 5342 0304 2874 2112 82

***Figure 9b:** Altered label. Return rerouted to a random address near the warehouse.*

4) Delivery

The hacked return label is placed on an empty parcel and shipped. When dropped off at a random address near the returns warehouse, the parcel receives a "Delivered" scan from the carrier. Since tracking data only shows the zip code, it is impossible to tell the exact location of the delivery or that the return has been sent to the wrong address.



Tracking Number:
7638287402197490281012

Latest Update

Your item was picked up at a postal facility at 5:20 pm on April 18, 2024 in LOS ANGELES, CA 92814.

Get More Out of USPS Tracking:

Delivered

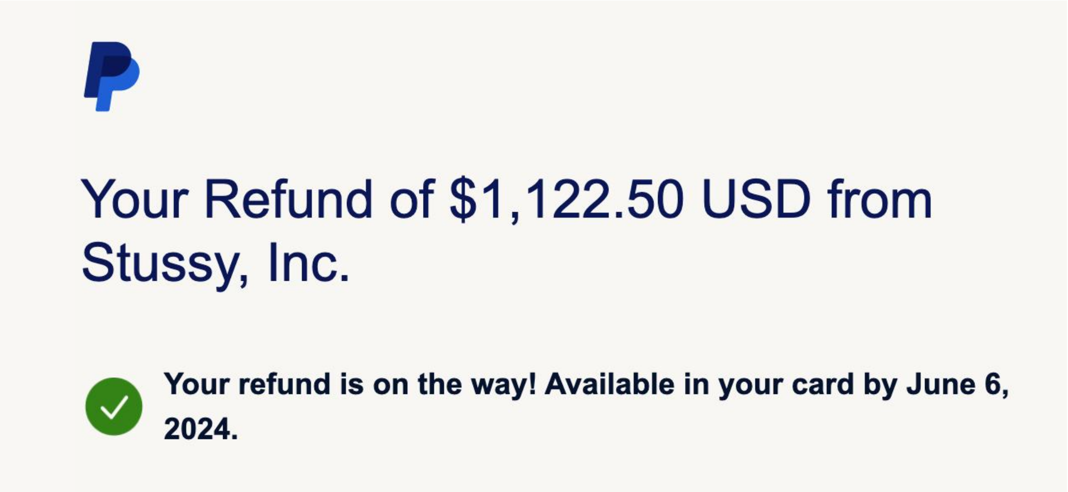
Delivered, Dropped In/At Mailbox
LOS ANGELES, CA 92814
April 18, 2024, am

Figure 10: *Fraudulent return tracking information is indistinguishable from normal delivery*

5) Profit

Once the return shows as delivered, the fraudsters can get their refund in 2 ways:

1. **Automatic Refund:** For retailers that process refunds based on *“delivered”* or *“in-transit”* tracking events, fraudsters have a frictionless environment they can exploit multiple times undetected.
2. **Manual Refund:** For retailers that manually process refunds upon receipt and inspection, fraudsters contact customer service citing that the tracking details show “delivered.”



Your Refund of $1,122.50 USD from Stussy, Inc.

✓ **Your refund is on the way! Available in your card by June 6, 2024.**

Figure 11: *Refund is processed upon “in-transit” or “delivered” carrier scans or is manually processed*

Why Rising D2C Brands are the Primary Targets of FTID Fraud

Overview

FTID fraud affects thousands of companies, but rising D2C brands, especially those that automate their return processes, are the primary targets. These brands don't have large dedicated fraud teams and can't possibly check details on every order or return for fraud. Furthermore, many D2C brands rely on 3PLs, adding to the lack of control over the returns process. This leads many brands to automate their returns, making them a prime target for fraudsters.

Automated Refund Processing

Due to resource limitations and a desire to maximize customer experience, rising D2C brands often automate their refunds to process upon certain tracking events like “In-Transit” or “Delivered.”

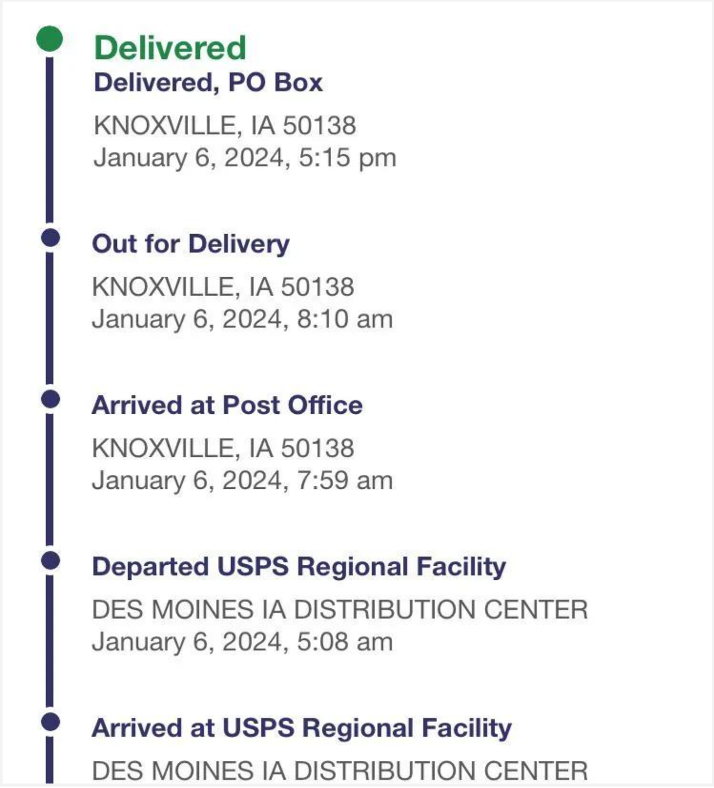
In FTID fraud, social engineering is required for brands manually checking returns, which introduces a risk of failure. On the other hand, brands automating returns have less signals of fraud to pick up on, often leaving FTID fraud to go on for years. A healthcare apparel brand we spoke to wasn't aware they were facing FTID despite being mentioned on Telegram fraud forums for over two years.

> Brands using automated refund platforms like **Loop Returns** and **Narvar** are prime targets for refund fraud. Fraudsters specifically target these retailers knowing they can get refunds without interacting customer service.

Why Manual Refund Processing Doesn’t Solve FTID

Manual refunds refers to when retailers issue refunds only upon receipt and inspection at the warehouse. Fraudsters exploit this system by contacting customer service and citing the tracking details that show “delivered” as proof when demanding a refund.

> We constantly get individuals that call demanding their refund. Even though many seem off, they show proof of delivery which forces our hand to issue a refund.
>
> *- Founder & CEO of a Jewelry brand*



Delivered
Delivered, PO Box
KNOXVILLE, IA 50138
January 6, 2024, 5:15 pm

Out for Delivery
KNOXVILLE, IA 50138
January 6, 2024, 8:10 am

Arrived at Post Office
KNOXVILLE, IA 50138
January 6, 2024, 7:59 am

Departed USPS Regional Facility
DES MOINES IA DISTRIBUTION CENTER
January 6, 2024, 5:08 am

Arrived at USPS Regional Facility
DES MOINES IA DISTRIBUTION CENTER

Figure 12: *Tracking events indistinguishable from a legitimate return.*

While manually checking returns can help customer service teams spot discrepancies in order history, this method raises operational costs and remains imperfect—fraudsters are skilled at mimicking legitimate customers, making it difficult to differentiate between the two. Furthermore, even legitimate packages occasionally get lost in the warehouse, forcing brands to make tough decisions between two significant risks:

1. **Denying an honest customer** a refund for a legitimate return.
2. **Issuing a refund to a fraudster**, creating a positive feedback loop within refunding communities.

The end result of successful FTID fraud is that the brand has paid return postage and issued a refund for an item they never receive, the fraudster has kept the merchandise, and the hacker has pocketed 10-20% of the value of the refund, a typical refund-fraud-as-a-service fee.

The Challenges of Combating FTID Fraud for Retailers

Overlooked Financial Drain

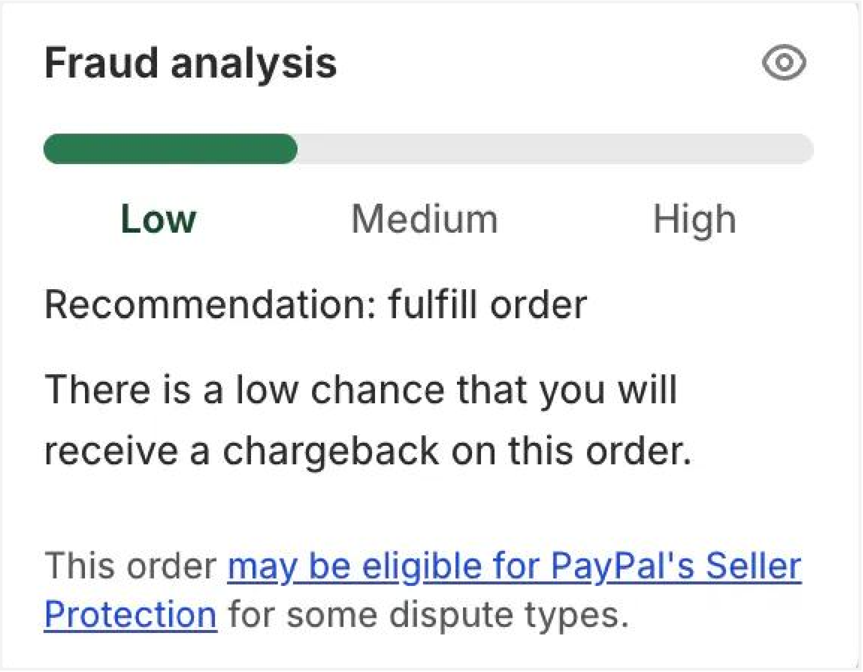
Tailed has engaged with dozens of retailers to gain a comprehensive understanding of FTID fraud, and most are unaware that it is even occurring within their operations. For many, FTID has persisted for so long that it has become a routine part of their financial operations.

Those that are aware often significantly underestimate its financial impact. Here's why it is so hard for brands to detect and combat.

Gaps in Existing Fraud Tools

Existing fraud detection tools built into **Shopify, Loop Returns,** and **Narvar** are inadequate for detecting FTID fraud.

Shopify's tool focuses on payment fraud, not return-related scams. Loop and Narvar rely on simple checks that fraudsters can easily bypass. These tools often misclassify fraudulent returns as "low risk," giving retailers a false sense of security.



Fraud analysis

Recommendation: fulfill order

There is a low chance that you will receive a chargeback on this order.

This order may be eligible for PayPal's Seller Protection for some dispute types.

Figure 10: *Shopify Risk Analysis Tool classifying an order as 'low risk'. FTID fraud was later used on the return.*

Operations Teams Stretched Thin

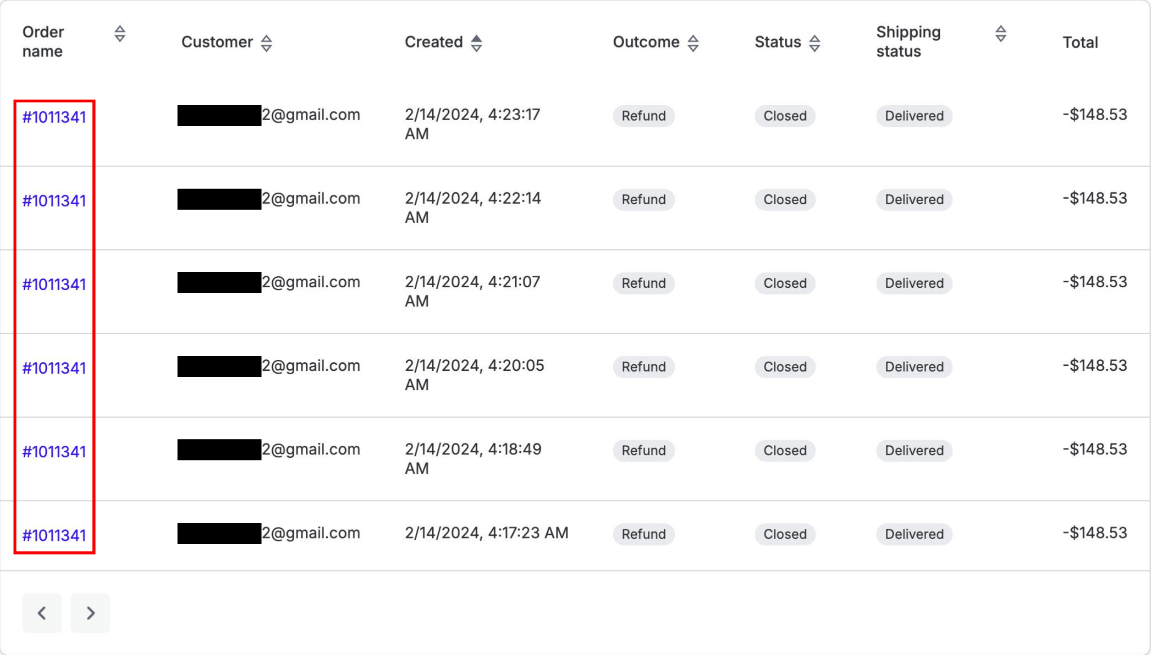
At the same time, rising D2C brands under $1 billion in revenue aren't equipped with large dedicated fraud teams or advanced fraud software that would create friction for fraudsters. Lean eCommerce teams juggling many responsibilities struggle to stay up to date with the wide range of fraud tactics used. In fact, a fraud analyst at one such brand admitted it was impossible to manually check every return due to the overwhelming volume of returns received every week.

Legal Action Falls Short

Legal action is rarely cost-effective for combating FTID fraud. When detected fraud amounts for an individual fraudster are less than $100K, the cost of pursuing legal action often exceeds potential recovery. Even large companies like Amazon, despite taking legal action against hundreds of fraudsters, still face significant losses.

Fraudsters Are Smart

Fraudsters are aware that retailers use manual workflows, such as dollar limits, to detect return fraud, and they test these limits before launching large-scale attacks on a brand. Tailed has observed fraudsters splitting orders and returns into smaller values to bypass these limits, as well as using VPNs and creating new emails to avoid order blockers. This makes it challenging for retailers to maintain effective fraud prevention, as fraudsters move on to new techniques before retailers can adjust.



Order name	Customer	Created	Outcome	Status	Shipping status	Total
#1011341	[redacted]2@gmail.com	2/14/2024, 4:23:17 AM	Refund	Closed	Delivered	-$148.53
#1011341	[redacted]2@gmail.com	2/14/2024, 4:22:14 AM	Refund	Closed	Delivered	-$148.53
#1011341	[redacted]2@gmail.com	2/14/2024, 4:21:07 AM	Refund	Closed	Delivered	-$148.53
#1011341	[redacted]2@gmail.com	2/14/2024, 4:20:05 AM	Refund	Closed	Delivered	-$148.53
#1011341	[redacted]2@gmail.com	2/14/2024, 4:18:49 AM	Refund	Closed	Delivered	-$148.53
#1011341	[redacted]2@gmail.com	2/14/2024, 4:17:23 AM	Refund	Closed	Delivered	-$148.53

***Figure 11:** A fraudster splits their order into multiple returns to bypass a merchant's fraud prevention workflow for returns over $400.*

Signs of FTID: How Retailers Can Spot the Threat

Empty Bubble Mailers

A clear sign of FTID fraud is receiving empty bubble mailers with manipulated return labels—instances where the carrier corrected the manipulated label and delivered it to the correct address. However, this is rare, and the absence of this signal does not mean FTID fraud isn't occurring.

High Value Orders Subsequently Returned

Fraudsters will often split returns into multiple smaller shipments to evade detection. If a customer returns all items from an order in separate shipments, this pattern should be closely monitored for potential fraud. In this instance, the best thing to do is delay issuing the refund until the package has been confirmed as received with your warehouse or 3PL.

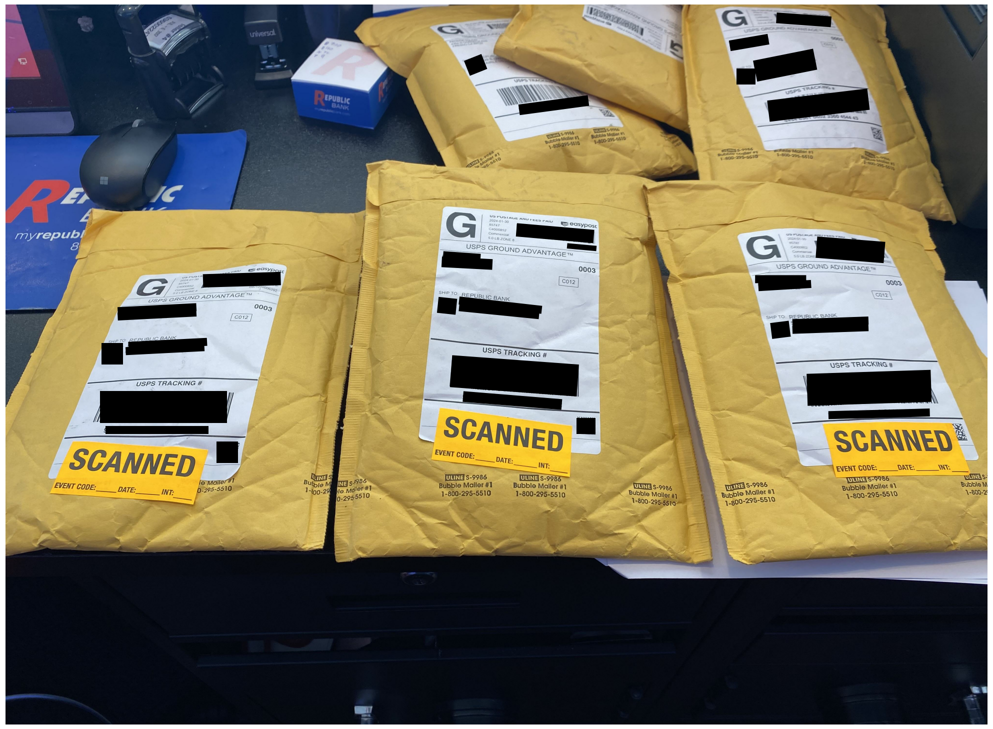
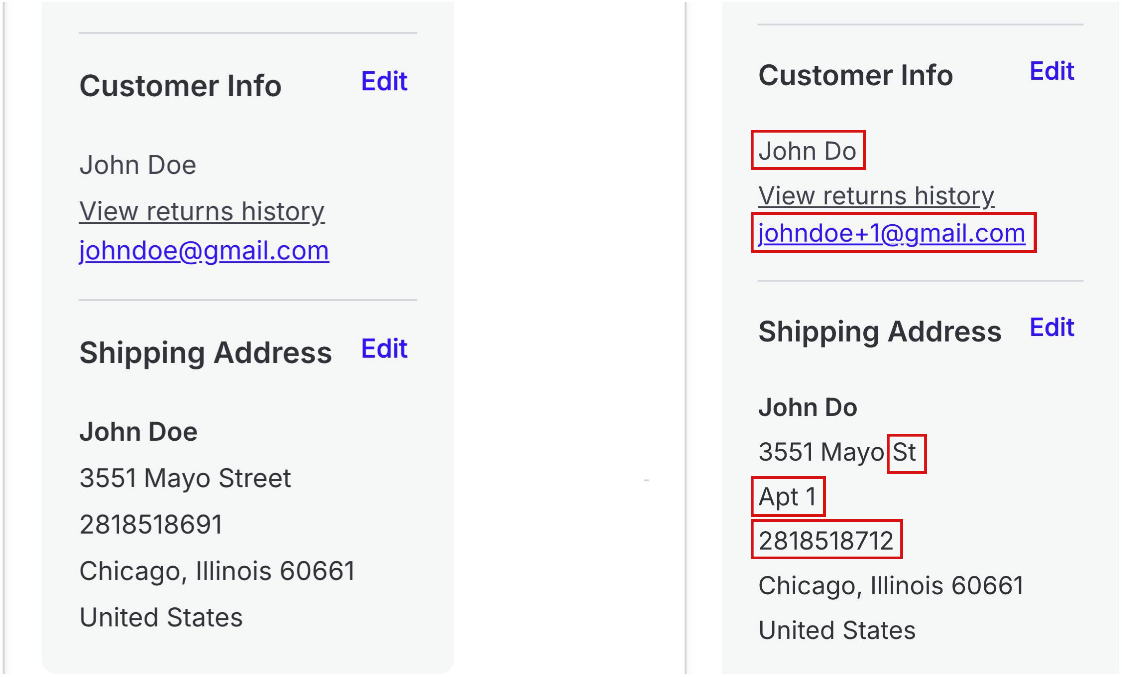


Figure 12: *BRUNT Workwear discovered return packages meant for their warehouse were rerouted to Republic Bank, a nearby business.*

A Footwear Brand only recovered three empty bubble mailers, but were on track to lose **over $500K** to FTID fraud that year.

Repeated Orders from New Emails and “Jigged” Addresses

A common tactic in FTID fraud involves creating new emails and slightly altering shipping addresses, known as "jigging," to bypass fraud detection systems. If there is a pattern of orders and returns from the same individual using variations of their email or address, it strongly suggests FTID fraud. This is particularly challenging to combat, as **each new email and jigged address can evade the filters and blocklists** set by your operations team.



Customer Info Edit

John Doe

View returns history

johndoe@gmail.com

Shipping Address Edit

John Doe
3551 Mayo Street
2818518691
Chicago, Illinois 60661
United States

Customer Info Edit

John Do

View returns history

johndoe+1@gmail.com

Shipping Address Edit

John Do
3551 Mayo St
Apt 1
2818518712
Chicago, Illinois 60661
United States

Figure 13a, 13b: *Fraudster jigs their address across two separate orders, changing the Name, Email, and Address settings. Though these are clearly the same person, jigging an address is enough to bypass many fraud risking tools.*

Note: Even if these specific signs aren’t immediately visible, it’s very likely that fraudsters are continually probing your brand for weaknesses. These indicators can surface suddenly and without notice, so maintaining a vigilant and proactive approach to fraud detection is essential.

Case Study: BRUNT Workwear

Background

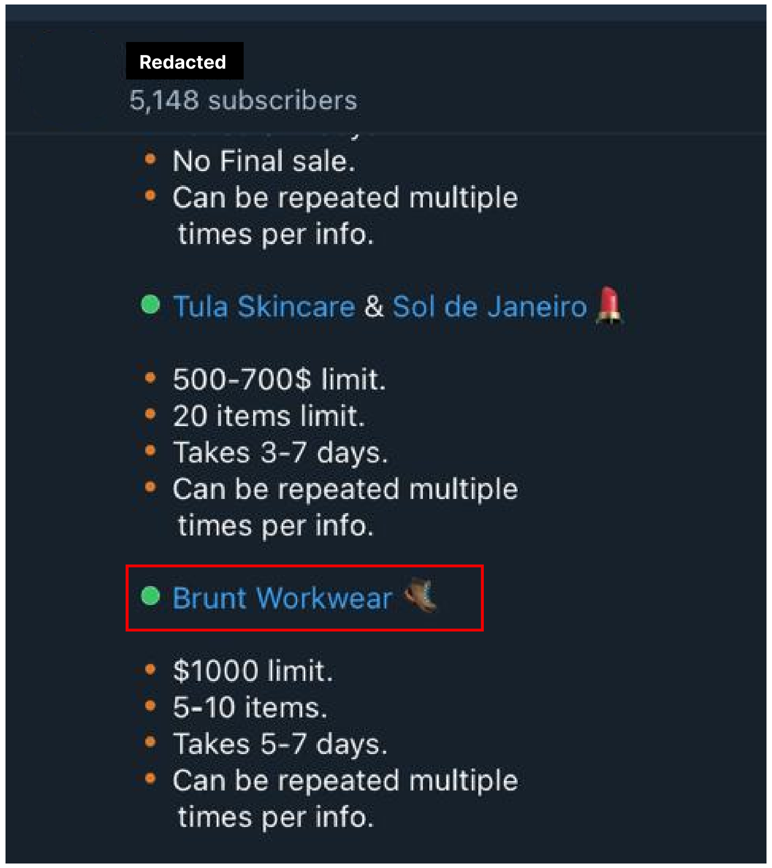
BRUNT Workwear uses **Loop Returns** to automate their refund processing—refunds are triggered once tracking information is updated to “delivered.” This allowed BRUNT to provide faster refunds to customers, ease logistics, and reduce the number of staff needed in warehouses.

The Fraud Wave

BRUNT encountered its first case of FTID fraud in April. After noticing an increase in large orders that were subsequently "returned," the operations team was contacted by a local bank reporting that dozens of empty mailers had been delivered to them, all listing "BRUNT Workwear" as the recipient.

Redirected Returns

The fraudster had selected the bank as the destination for the manipulated return shipping labels. Fraudsters often select locations like restaurants, hotels, or businesses— where they expect incorrectly delivered items to be discarded—as the delivery address for manipulated labels, to minimize the risk of detection.



Redacted
5,148 subscribers

- No Final sale.
- Can be repeated multiple times per info.

● Tula Skincare & Sol de Janeiro

- 500-700$ limit.
- 20 items limit.
- Takes 3-7 days.
- Can be repeated multiple times per info.

● Brunt Workwear

- $1000 limit.
- 5-10 items.
- Takes 5-7 days.
- Can be repeated multiple times per info.

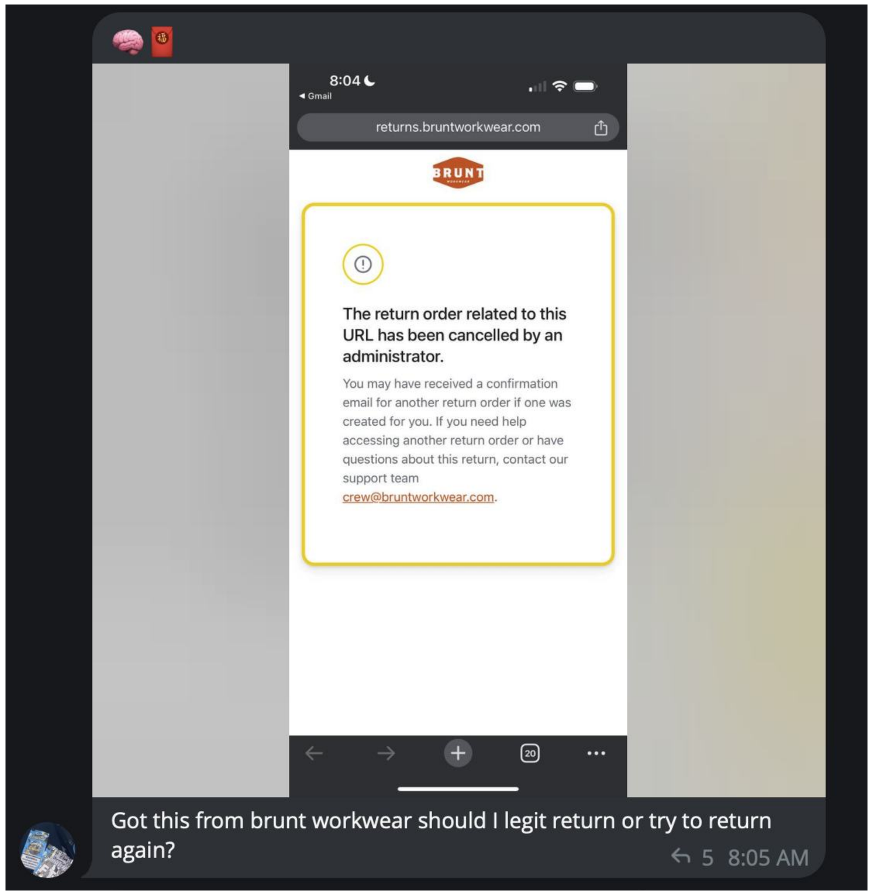
Figure 14: *BRUNT Workwear advertised as vulnerable to FTID fraud in a refund fraud forum. The method of fraud, order/item limit, and refund settings are shown.*

Stopping the Fraud Wave

At one point, **5.7% of all BRUNT's returns** were subjected to FTID fraud. Keyword mentions of "BRUNT" skyrocketed, increasing 1,720% from the previous month.

> The team at Tailed was able to stop $20K in fraud the first week we worked with them. Without implementing them, we would've been looking at over $500K in losses.
>
> ***- Emily H, Operations Manager at BRUNT Workwear***

BRUNT chose Tailed for our comprehensive fraud database and proven track record. Within 24 hours, Tailed was integrated, and in **BRUNT's first week addressing the issue, $21,081 in fraudulent returns were flagged**. The following three weeks saw sequentially reduced amounts of fraud. Just as fraud vouches lead to a positive feedback loop of fraud, a negative loop can be created by other fraudsters writing warnings that their fraud attempts on a specific brand failed. Five months later, **the true fraud rate was confirmed to be zero** for the entire month of August, after confirming with BRUNT's Operations team that all returns had been received.



The return order related to this URL has been cancelled by an administrator.

You may have received a confirmation email for another return order if one was created for you. If you need help accessing another return order or have questions about this return, contact our support team crew@bruntworkwear.com.

Got this from brunt workwear should I legit return or try to return again?

Figure 14: *A fraudster asks others in the refunding community for advice on what to do after Tailed denies their refund.*

About Tailed and How We Can Help

In today's eCommerce environment, businesses face increasing risks from sophisticated fraud schemes like FTID. Implementing a solution such as Tailed can help protect your brand by seamlessly integrating with your existing returns system to detect suspicious patterns and discrepancies in return data. Tailed enables brands to continue automating returns while preventing fraudulent activity and ensuring legitimate returns are processed smoothly.

How Tailed Can Help:

- **Real-Time Returns Monitoring:** Tailed analyzes every transaction to flag potential fraudulent returns, blocking their refund and providing actionable insights for your customer service team.
- **Identity Linking:** Tailed has the largest database of refund fraudsters. Using advanced fingerprinting, Tailed creates identity groups to link personas back to the real fraudster, preventing them from changing their address or making new emails to bypass your existing fraud tools.
- **Returns Audit:** Tailed offers a complimentary audit of your last 120 days of returns, providing a detailed report on past fraudsters and insights into potential vulnerabilities.

Retailers using Tailed have seen significant reductions in FTID fraud. An apparel brand **reduced their FTID fraud rate from 14.3% of all returns to 0%** after integrating Tailed. Their fraud analyst confirmed that manually checking every return was not feasible, and that Tailed's automation has made this process more efficient, saving both time and resources.

If you're interested in learning more about preventing FTID fraud or getting a free analysis of your exposure, feel free to reach out to us at contact@tailed.ai or visit us at tailed.ai.