Whitepaper

Return Fraud Guide

Agilence

Agilence

Table of Contents

Agilence

Return Fraud Guide

According to the US-based National Retail Federation, return fraud has ballooned into a $101 billion issue, affecting a staggering 13.7% of all returns in the US in 2023. In the United Kingdom, the UK retail industry lost £11.3 billion ($14.3 billion) due to fraudulent returns, according to the Centre for Economic Business and Research.

For loss prevention and asset protection professionals, as well as operations and retail managers, understanding and combating this pervasive problem is critical for safeguarding profits and maintaining operational efficiency. In this comprehensive guide, we explore essential topics such as the definitions and impact of return fraud, the common types of fraudulent returns, and the connection between organized retail crime and return fraud. You will also find practical steps to prevent return fraud and insights into how modern technology can be used to fight back.

What is Return Fraud?

Return fraud is a set of unethical practices where individuals (or organized groups) exploit a retailer's return policies for their own gain at the expense of the retailer. These fraudulent activities impact retailers by causing financial losses, damaging inventory accuracy, and undermining customer trust.

A recent Loop survey found:

- **91% of UK retailers experienced an increase in fraudulent returns or policy abuse over the past 12 months.**
- **64% of UK retailers identified returns fraud as their biggest challenge.**
- **38% of UK online shoppers engaged in or knew someone who engaged in return policy abuse in the past 12 months.**
- **27% of respondents admitted to "wardrobing," 17% exploited lenient return policies, 59% made a return to determine fit or sizing.**

Agilence

Return Fraud vs. Refund Fraud vs. Refund Abuse What's the Difference?

There are many different terms used to describe this range of practices, including return or returns fraud, retail return fraud, return abuse, refund fraud and refund abuse. Subtle distinctions between these terms reflect differences in the legality and specificity of these acts.

Return Fraud

Return fraud involves the act of returning a product or requesting a refund when the product does not qualify for either. It specifically targets retail return policies, which might require a receipt or the original packaging. For instance, a person might falsely claim that an item is damaged or unsatisfactory to secure a refund or replacement, even though the product is in good condition. The goal here is to exploit customer-friendly return policies to gain undeserved benefits.

Unlike many other types of fraud, return fraud often exists in a grey area. It is perpetrated by fraud rings, crime syndicates, and hardened hackers. In fact, an entire industry has emerged of fraudsters specialising in return fraud, fake tracking IDs (FTIDs), and empty boxing methods and services. But it is also done by regular shoppers who may be law-abiding citizens in any other aspect of their lives and good customers outside the occasional illegitimate refund.

Refund Fraud

Refund fraud is a broader term that encompasses any scam aimed at obtaining unwarranted refunds or reimbursements from companies, governments, or financial institutions. While return fraud falls under this category, refund fraud extends beyond retail settings. It includes fraudulent activities such as tax refunds, chargebacks, and insurance reimbursements. Essentially, refund fraud involves making false claims about an item or service to receive a monetary refund without returning the product in question.

Refund Abuse

Return or refund abuse, often seen as less severe than fraud, includes behaviour that exploits return policies without breaking the law to the same degree. This can involve practices like "bracketing," where customers buy multiple sizes or colours of a product and return the ones they don't want, or "wardrobing," where items are used once and then returned, which we describe in more detail below. These actions, while not illegal, still lead to significant losses for retailers.

Analyst house GlobalData revealed that in 2022, the value of online clothing returns made by UK shoppers exceeded GBP £4.1 billion. Predictions suggest this figure will increase by 16.7% by 2027.

45% of shoppers in the UK have admitted to return fraud or policy abuse, meaning $22.8 billion in return-based fraud was estimated in 2022.

Agilence

The Impact of Return Fraud on Retailers

Return fraud poses a significant challenge for retailers, resulting in substantial financial losses and operational disruptions. Data shows that retailers incur $166 million (£130 million / €150 million) in merchandise returns for every $1 billion (£785 million / €905 million) in sales and lose approximately $10.40 (£8.15 / €9.40) to return fraud for every $100 (£78.50 / €90.50) of returned merchandise accepted. This translates to an estimated $24 billion (£18.85 billion / €21.7 billion) in annual losses.

The problem intensifies during peak shopping periods, particularly the festive season, when 25% of annual product returns occur. During this time, attempts at e-commerce fraud also surge, with TransUnion reporting that fraud attempt rates during the holidays in 2022 were 82% higher globally compared to the rest of the year.

Beyond the financial hit, return fraud can erode customer trust and tarnish a retailer's reputation. When businesses tighten return policies to combat fraud, they risk alienating legitimate customers who may become hesitant to make purchases out of fear that their genuine returns might not be accepted. This shift can lead to a decline in sales and damage to the brand's credibility. Return fraud creates a tricky tightrope for retailers to walk between providing a good customer experience on the one hand and ballooning inventory loss on the other.

Inventory Management Challenges

Return fraud also wreaks havoc on inventory management. Fraudulent returns create discrepancies between recorded inventory and actual stock levels, making it difficult for retailers to maintain accurate inventory records. This misalignment can result in overstocking or understocking issues, leading to either excess inventory storage costs or missed sales opportunities due to insufficient stock. One study found that retailers lose approximately 5-10% of their sales due to inventory inaccuracies caused by return fraud.

Moreover, processing fraudulent returns consume valuable time and resources, diverting attention from managing legitimate inventory needs. The complications extend to warehousing and logistics, where additional steps are required to verify the authenticity and condition of returned items. These inefficiencies can slow down operations and increase overall handling costs. According to Deloitte, 10% of all supply chain costs are now dedicated to reverse logistics, which includes handling fraudulently returned items.

eCommerce Return Abuse

Returns, legitimate or not, are already costly for retailers. On average, returns cost retailers nearly 60% of the item's original sales price, placing a severe financial burden. When return abuse happens online in an e-commerce transaction, costs rise even higher.

Processing an online return is already a costly proposition, averaging 21% of an order’s value, according to a Pitney Bowes survey of 168 retailers (half the respondents paid more than 21%). As shipping and processing costs have been rising, the costs of processing returns grow as well, adding an extra layer of loss on even ‘harmless’ refund abuse.

As retail shifts increasingly online, the dynamics of return fraud evolve. Approximately 38% of merchants have reported a rise in buy-online, return-in-store (BORIS) transactions, with 29% noting an increase in fraudulent returns within these transactions.

The ongoing battle against return fraud requires strong loss prevention strategies to safeguard both the business's financial health and its relationship with honest customers.

Agilence

Types of Return Fraud

Return fraud can take various shapes and forms, each presenting unique challenges for retailers. Here's a detailed look at some of the most common types of return fraud.

Wardrobing

Also known as "renting," wardrobing involves purchasing an item, using it briefly (often for special occasions), and then returning it for a full refund. This practice exploits generous return policies. For example, a customer might buy an expensive dress for a wedding, wear it once, and then return it the next day claiming it was never worn. Retailers often struggle to prove an item has been used, leading to significant financial losses. In some cases, shoppers effectively ‘rent’ clothing for free over an entire season, purchasing items and returning them at the end of a fashion cycle.

Wardrobing accounts for approximately 50% of all return fraud. A survey by Forter found that 56% of consumers admitted to wardrobing, and one in four shoppers said they bought an item during the 2023 holiday season with the intention of returning it after use. Nearly half of those engaging in wardrobing were aged 18 to 34.

A milder form of this behaviour is “bracketing,” where a shopper buys multiple sizes or colours of an item with the intent of returning whichever doesn’t fit. A more blatant type of return fraud, similar to wardrobing, is switch fraud or the “upgrade scam,” where a customer purchases a new version of a product they already own and returns their old, used item in its place for a refund. In some cases, scammers then resell the new product for profit. Despite its name, wardrobing isn’t limited to clothing. It frequently occurs with tools, appliances, and other high-value equipment, which are purchased for a one-off project and then returned after use, effectively serving as a free rental. This is particularly common with items that are expensive and only needed temporarily.

Returning Stolen Goods

A more serious form of return fraud involves returning stolen goods—where an individual steals merchandise from a store or obtains it illegally and then attempts to return it for cash, a voucher, or store credit. This is a straightforward case of fraud, with the offender seeking financial gain by converting stolen goods into money or in-store value.

One common method involves a thief stealing items and then using a third party—such as a friend, acquaintance, or even a stranger—to return them to the store. This tactic helps the thief avoid direct involvement in the return process, where retailers often request identification or proof of purchase. Many retailers in the UK and EU now implement stricter return policies, such as requiring receipts or tracking previous return patterns, to prevent this type of fraud.

E-commerce Fraud

Return fraud isn’t limited to physical stores—it also affects online retailers. A common scam involves false claims of non-delivery, where a customer reports that an order never arrived (e.g., stolen from a shared building entrance or lost by a courier) and requests a refund or replacement. Fraudsters exploit retailer policies designed to ensure customer satisfaction, ultimately keeping both the refunded amount and the product.

Other forms of e-commerce return abuse include excessive refund requests or serial returns. Retailers can mitigate this by tracking return behaviour and identifying suspicious patterns. The Agilence eCommerce Module helps businesses detect and prevent fraudulent returns by analysing transaction data and pinpointing high-risk activity.

Agilence

Types of Return Fraud

Receipt Fraud

Receipt fraud occurs when fraudsters alter, forge, or misuse receipts to obtain a refund for more than the original purchase price or return items they never actually bought. A common tactic involves using found, counterfeit, or stolen receipts to deceive retailers into issuing refunds.

For example, an individual might find a receipt in a car park, purchase the same item from another retailer, and then return it using the found receipt to claim a refund. This tricks the retailer into giving money back for merchandise that was never purchased from their store. Organised criminal groups may also forge receipts in bulk and commit this type of fraud across multiple store branches.

Receiptless returns present another challenge. Some customers return items claiming they lost the receipt—this could be a genuine mistake or an attempt to exploit lenient return policies. Another method of abuse is multiple returns using a single receipt. A fraudster may use the same receipt to return multiple versions of an item across different store branches, often involving stolen goods. Verifying the authenticity of the return and ensuring it matches the original purchase price—especially when discounts, sales, or promotions were applied—can be difficult.

Receiving a Refund Greater than Purchase Price

Receiptless returns sometimes allow customers to receive a refund that exceeds the amount they originally paid. Some retailers issue refunds based on the current selling price of an item if a receipt isn't provided, which means that a customer who bought an item at a discount could return it later and receive a full-price refund, or a fraudster could exploit price fluctuations and return items when prices are highest, profiting from the difference.

To prevent this, many retailers use a Lowest Offered Price Lookup System, which checks the lowest price at which the item was sold during a set period (e.g., the last 90 days) and issues the refund accordingly. This protects against fraudulent returns while maintaining fair customer service standards.

Bricking

Bricking occurs when fraudsters tamper with electronic products before returning them, rendering the item useless ("bricked"). For example, a customer may buy a smartphone or laptop, remove valuable components like the battery, processor, or screen, replace them with non-functional parts, and then return the item claiming it is faulty. They then resell the valuable parts for profit while still receiving a full refund from the retailer. While many UK and EU retailers track serial numbers or IMEIs to prevent fraud, some fraudsters find ways to bypass these controls—especially if the item is returned to a different store location or if the retailer does not thoroughly inspect returns.

Cross-Retailer Returns

Cross-retailer returns involve returning a product to a different retailer than where it was originally purchased to exploit price differences and refund policies. A common example is a customer who buys a pair of shoes from a discount retailer and returns them to a premium retailer with a more lenient return policy to claim a higher refund. Another version of this fraud occurs when a product is purchased on sale or with a promotion and later returned at full price, allowing the fraudster to profit from the price difference.

While some cross-retailer returns may be accidental, they become fraudulent when done deliberately to exploit pricing and return policy differences. This type of fraud can be difficult to detect, as the returned product may be identical to what the retailer sells, making it hard to verify where it was originally purchased. Some UK and EU retailers mitigate this risk by requiring proof of purchase or implementing price-matching policies that limit return fraud.

Agilence

Types of Return Fraud

Empty Box Scam

Like wardrobing, the empty box scam is a common form of e-commerce return fraud. Customers return empty boxes or fill them with worthless items instead of the original product. Fraudsters have scammed major UK and EU retailers, including Amazon and ASOS, for millions. Some alter shipping details to make tracking difficult or falsely claim they received an empty box. Since many retailers offer prepaid return labels, fraudsters exploit automated return processes to avoid detection.

Product Not Present Returns

Customers claim a product was defective (e.g., spoiled food) and seek a refund without returning the item. Verifying claims without physical evidence is difficult, making perishable goods and cosmetics vulnerable. UK and EU retailers now request photo evidence or partial returns (e.g., bottle caps, empty packaging) to prevent abuse while complying with consumer rights laws.

Employee Fraud

Internal refund fraud occurs when employees manipulate the refund process for their own gain. This could involve issuing fraudulent refunds to their own accounts, collaborating with external fraudsters in exchange for a cut of the money, or creating fake returns for products that were never sold. Retailers combat this with CCTV monitoring, POS tracking, and real-time audit logs to flag suspicious refund activity. Mystery shoppers and data analytics also help detect unusual refund patterns.

Gift Card Fraud

Gift card fraud involves returning stolen or fraudulently obtained goods in exchange for store credit or gift cards, which are then sold or converted into cash through third-party platforms. Fraudsters may also use self-service kiosks to exchange gift cards for money.

Since gift cards are less regulated than bank transactions, they are a preferred method for fraudsters to launder money or offload stolen goods. Some UK and EU retailers are implementing enhanced tracking for gift card transactions, requiring proof of purchase for store credit refunds, or imposing refund delays to limit abuse.

Cheque and Credit Card Fraud

Fraudsters may use bounced cheques or stolen credit card details to make fraudulent purchases and then attempt to return the items for cash or store credit before the retailer realises the payment was invalid. This form of fraud exploits the time gap between the fraudulent transaction and the bank's detection process.

To counter this, UK and EU retailers increasingly use real-time payment verification systems, apply stronger fraud filters for high-value purchases, and delay refunds until the original payment clears. Chip & PIN and 3D Secure authentication (such as Verified by Visa and Mastercard SecureCode) have also helped reduce some credit card fraud cases in Europe.

Additionally, some fraudsters buy high-value items with stolen credit cards, return them, and attempt to get the refund credited to a different account. While less common than cash or store credit fraud, some retailers flag mismatched payment details and require refunds to be processed to the original payment method only.

Agilence

ORC and Returns Fraud Abuse

Return fraud isn't limited to opportunistic shoppers—Organised Retail Crime (ORC) groups are increasingly using coordinated, large-scale tactics to exploit retail return policies for financial gain. These groups steal bulk merchandise from stores, distribution centres, or hijacked shipments, then return the goods across multiple retailers and locations without receipts to obtain store credit or gift cards. These are then sold online, laundered through third-party marketplaces, or converted into cash via resale platforms and kiosks.

Unlike individual fraudsters, ORC groups operate across regions and even countries, making detection and prevention a significant challenge for UK and EU retailers. Their tactics evolve to exploit loopholes in return policies, often using fake identities, fraudulent receipts, or third-party intermediaries to obscure their tracks.

To combat ORC-related return fraud, retailers must tighten return policies, invest in AI-driven analytics like Agilence Analytics, and leverage real-time fraud detection tools. Additionally, greater data-sharing across retailers and closer collaboration with law enforcement agencies can help identify and dismantle these criminal networks, mitigating their financial and operational impact on the retail sector.

Signifyd data shows that in Europe there was a 35% increase in false claims that an item never arrived in 2022, and a 68% increase in false claims about the condition of a product.

How to Prevent Return Fraud: 10 Key Steps

Preventing return fraud requires a strategic approach combining stringent policies, employee training, and advanced technology. Here are ten actionable steps retailers can implement to reduce the risk of fraudulent returns, protect profits, and enhance overall store security. From establishing robust return policies to leveraging technology to track suspicious activities, these measures provide a comprehensive framework for tackling this costly issue.

1. **Implement a Robust Return Policy**: Establish clear and strict return policies that are prominently displayed both in-store and online. Specify conditions such as time limits for returns, the need for original receipts, and the state of merchandise (e.g., unused, with tags attached). Ensure staff are trained to consistently enforce these policies.

2. **Require Identification for Returns**: For returns without a receipt, require a valid photo ID (e.g., passport, driving licence). This helps create a record of the transaction and can deter fraudulent activity by making it easier to track and identify repeat offenders.

3. **Employ a Lowest Price Refund Policy**: When processing non-receipted returns, use a system that refunds customers based on the lowest price the item was sold for during a specified period (e.g., the last 90 days). This prevents fraudsters from exploiting pricing discrepancies to gain higher refunds than what was originally paid.

Agilence

How to Prevent Return Fraud: 10 Key Steps

4 **Monitor Gift Card Transactions:** Keep a close eye on gift card purchases and redemptions. Implement measures such as limiting the amount that can be loaded onto a gift card and requiring additional verification for high-value transactions. Collaborate with third-party marketplaces to track and flag suspicious activities involving your store's gift cards.

5 **Educate and Train Employees:** Conduct regular training sessions for employees to help them recognise signs of return fraud and understand the importance of adhering to established return policies. Empower them to question suspicious returns and escalate issues to management when necessary.

6 **Enhance Receipt Verification:** Adopt advanced receipt verification technologies, like barcodes or QR codes, which can be scanned to validate purchase details quickly and accurately. This can prevent the use of counterfeit receipts in return fraud.

7 **Limit Cash Refunds:** Where possible, limit cash refunds and offer store credits instead. This can deter fraudsters who are primarily interested in converting returned merchandise into cash.

8 **Collaborate with Other Retailers:** Join retail associations or networks that share information on return fraud trends and known offenders. Collaborative efforts can lead to industry-wide strategies and more robust defences against fraudulent activities.

9 **Regularly Review and Update Policies:** Continuously review and update your return policies and procedures to adapt to new fraud tactics. Stay informed about the latest trends in return fraud and adjust your preventive measures accordingly.

10 **Use Technology to Track Returns:** Invest in software tools that track return patterns by customer, product, and location. This can help identify suspicious activity, such as frequent returns by the same customer or high return rates for certain products. We explore this more in the next section.

Fighting Return Fraud with Technology

When it comes to combating return fraud and abuse, there's no one-size-fits-all solution. Retailers need to employ a variety of strategies and technologies to achieve the best results. Returns management software, such as a real-time returns authorisation tool, is an essential part of the solution. These tools use rules- or score-based systems to provide immediate feedback at the point of sale, informing the cashier whether a return can be processed. Rules-based systems enforce customer policies, such as no returns on items with receipts older than a specific period, while score-based systems assign a score to each customer based on their previous behaviour to help make return authorisation decisions.

However, a real-time authorisation or returns management solution on its own is not enough, as it may lack a broader analytical context to identify trends and patterns or link returns data to other customer behaviours and operational data sources. This is where a tool like Agilence Analytics excels. While returns authorisation tools are critical for real-time operational decisions in retail, integrating an advanced analytics solution like Agilence can provide the deeper insights and broader analysis needed for strategic decision-making and effectively reducing shrinkage.

Neiman Marcus

Identified $960k worth of shrink in one year by targeting fraudulent refunds using Agilence Analytics

Agilence excels in identifying broader patterns and trends beyond real-time decisions, integrating data from returns authorisation systems with other data sources to provide deeper insights into return patterns, cashier behaviours, and customer profiles—all while offering a more accessible and intuitive interface with a robust alert system.
Here are some of the key indicators users can view in Agilence Analytics to help detect and prevent return fraud:

- Non-receipted Same-day Returns
- Same-day, Same-cashier Returns
- Returns Outside of Policy
- Net Negative Transactions
- Returns to a Different Tender Type
- Product Not Present Returns
- Return Reason Codes
- Store Credit and Employee Discounts
- Cashier's Last Name or Address Matches the Customer's

To learn about how Agilence Analytics can help your business fight return fraud and abuse, schedule a demo today!

About Agilence

Agilence is the leader in loss prevention analytics, helping prominent retail, restaurant, and grocery companies increase their profit margins by reducing preventable loss.

At Agilence, we specialise in uniting digital and physical transactions to help cutting-edge loss prevention teams expand beyond traditional theft and fraud to tackle preventable loss in all its forms – in-store, online, and at the corporate office.

Every day, Agilence analyses over 24 million transactions for our customers, transforming data into insights, and insights into actions. Our platform combines data from 200+ sources, including point-of-sale (POS), eCommerce, HR, labour, inventory, product, third-party delivery platforms, alarms, case management, loyalty, access control, video surveillance, and more.

Companies have saved millions of pounds by optimising operations, identifying sources of margin erosion, and reducing shrink using Agilence. Many have also improved employee and customer safety, identified training opportunities, enhanced customer experiences, increased promotional success, and eliminated productivity gaps.

Visit Agilenceinc.com to learn more.

Agilence