5 Steps Retailers Should Take to Mitigate Return Fraud

Retailers lose $23B[1] in fraudulent returns annually, and fraudsters stole 3.6%[2] of all e-commerce revenue in 2022. With forecasted growth of $500B from 2023 to 2027[3], it's raising even more concern that fraudsters can harness fraud to find vulnerabilities at the scale in an industry that is growing, especially with returns and customer service as a top element for success. It's pretty sad, but an astonishing 14%[4] of returns are fraudulent.

So what can retailers do about it to catapult growth while not sacrificing revenue losses to fraudsters? This guide lays out five simple steps that can help.

But first—what is **Return Fraud?**

Concession (or Return Fraud) Abuse is a growing scam service in underground forums that defrauds online retailers through the systemic abuse of their return policies. It's a way that fraudsters in retail, in particular, can exploit loopholes in company protocols or, in many cases, just good customer service, which is a tenant to any strong e-commerce business. Many of these fraud cases are socially engineered with generative AI and new platforms that make it easier for imposters to replicate audio and video to get through call centers quickly.

Step 1 | Rethink how to safeguard against return fraud

Many fraudsters get in by targeting concession abuse of online retailers and exploiting the returns process. By socially engineering the contact center agent, many can easily receive a free replacement or even a refund. As technology has progressed, organized attacks have become more common. Knowing they can get away with fraud creates a repeatable engine to further impact losses. There is an ecosystem, also referred to as the Concession Abuse as a Service (CAaaS), that consists of 2,251 "service providers" and growing who are adept at abusing returns.[5]

[1] NRF survey on Cost of Retail Returns 2022
[2] Developing a Framework for Understanding and Measuring E-commerce Losses in Retailing, 2023
[3] Statista, revenue of the e-commerce industry in the U.S. 2017-2027
[4] ECR Community Buy Online, Return in Store, The Challenges and Opportunities of Product Returns in a Multichannel Environment, 2019
[5] https://www.usenix.org/system/files/sec21-sun-zhibo.pdf

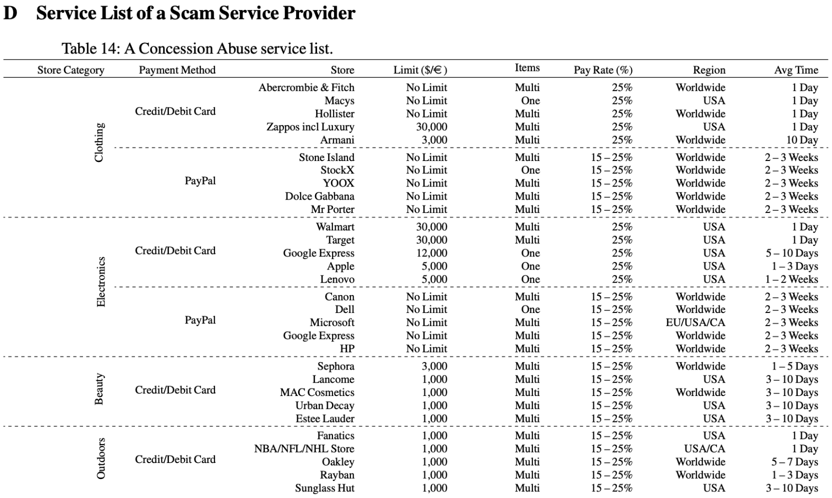
Step 2 | Understand how fraudsters think through the CAaaS system

Thinking from the angle of fraudsters allows you to safeguard and rethink the areas they are getting into. Here's how they work through a CAaaS system.

1. **Target:** Large merchants have robust customer service departments and are more willing to risk a financial loss in exchange for customer satisfaction. Fraudsters have identified certain companies willing to take such risks.
2. **Pinpoint**: Fraudsters prefer shopping accounts with more extended order history and fewer refund and return claims because those accounts resemble loyal customers. Consequently, they are more vulnerable to fraudsters' methods of replicating and exploiting those key accounts.
3. **Seek**: Compromised accounts with recent orders often allow refund requests. Fraudsters look at which recent orders appear routine to agents to avoid further scrutiny when looking for a path of least resistance.

Step 3 | Spotcheck the universal fraud database

Fraudsters have created detailed returns and abuse profiles of top retailers. Around 40 retailers from various categories, from electronics to clothing, home decor, and even pet foods, are all on these fraudsters' target lists. The CAaaS has a list of 264 retailers in its crosshairs and a good understanding of their return policies and tactics.



D Service List of a Scam Service Provider

Table 14: A Concession Abuse service list.

Store Category	Payment Method	Store	Limit ($/€)	Items	Pay Rate (%)	Region	Avg Time
Clothing	Credit/Debit Card	Abercrombie & Fitch	No Limit	Multi	25%	Worldwide	1 Day
		Macys	No Limit	One	25%	USA	1 Day
		Hollister	No Limit	Multi	25%	Worldwide	1 Day
		Zappos incl Luxury	30,000	Multi	25%	USA	1 Day
		Armani	3,000	Multi	25%	Worldwide	10 Day
	PayPal	Stone Island	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		StockX	No Limit	One	15 – 25%	Worldwide	2 – 3 Weeks
		YOOX	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		Dolce Gabbana	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		Mr Porter	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
Electronics	Credit/Debit Card	Walmart	30,000	Multi	25%	USA	1 Day
		Target	30,000	Multi	25%	USA	1 Day
		Google Express	12,000	One	25%	USA	5 – 10 Days
		Apple	5,000	One	25%	USA	1 – 3 Days
		Lenovo	5,000	One	25%	USA	1 – 2 Weeks
	PayPal	Canon	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		Dell	No Limit	One	15 – 25%	Worldwide	2 – 3 Weeks
		Microsoft	No Limit	Multi	15 – 25%	EU/USA/CA	2 – 3 Weeks
		Google Express	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		HP	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
Beauty	Credit/Debit Card	Sephora	3,000	Multi	15 – 25%	Worldwide	1 – 5 Days
		Lancome	1,000	Multi	15 – 25%	USA	3 – 10 Days
		MAC Cosmetics	1,000	Multi	15 – 25%	Worldwide	3 – 10 Days
		Urban Decay	1,000	Multi	15 – 25%	USA	3 – 10 Days
		Estee Lauder	1,000	Multi	15 – 25%	USA	3 – 10 Days
Outdoors	Credit/Debit Card	Fanatics	1,000	Multi	15 – 25%	USA	1 Day
		NBA/NFL/NHL Store	1,000	Multi	15 – 25%	USA/CA	1 Day
		Oakley	1,000	Multi	15 – 25%	Worldwide	5 – 7 Days
		Rayban	1,000	Multi	15 – 25%	Worldwide	1 – 3 Days
		Sunglass Hut	1,000	Multi	15 – 25%	USA	3 – 10 Days

Have you ensured your company isn't on this list? Have you looked at other companies that are targeted and why?

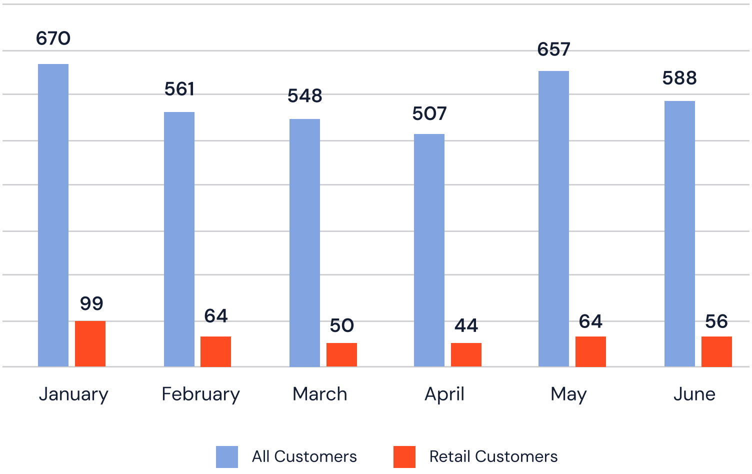
Access the link here to find out[6].

[6] https://www.usenix.org/system/files/sec21-sun-zhibo.pdf

Step 4 | Consider tech to help protect your call centers

Retail fraud calls are 7X higher than in other sectors[7]. The contact center is the final stage in mitigating concession abuse fraud. Agents employ steps to create friction during the return process, but various fraud specialists in the CAaaS ecosystem find ways to bypass these methods. That's why it's critical to have tech that keeps records for you.

According to Pindrop Labs, one in 99 calls at large US retailers are fraudulent, 16 times the average across all other sectors.



Step 5 | Protect call center agents from burn out

Here are the reasons why call centers are most vulnerable to fraudsters:

1. Fraudsters try many other channels, but the primary way of entry they prefer is by phone
2. Their goal is to give the agent less time to respond, making it harder to spot unusual behaviors and patterns
3. Social engineering passes through call centers more frequently

Automation and AI-based technologies in the call center will continue to increase over the next 5-10 years. Ensuring a good customer and employee experience without letting fraud pass through will be paramount. Since call centers aren't going anywhere, keeping them secure while providing a good customer experience will help set your company apart.

[7] Pindrop Labs analysis of fraud call rates at contact center agent leg

Conclusion

Agent communication with customers is crucial. Over 60% of all customer interactions are through the agents on live telephone calls.[8]

Personal connections and good experience remain at the center of business in retail. But it can come at the detriment of allowing fraudsters to take advantage. With the right plan and technology, you can easily safeguard against this. The goal will remain to proactively stop return fraud from happening by leveraging multi-factor fraud detection software. Be sure your company is ready as business scales.

See how a top US retailer generated 5X ROI by implementing Pindrop fraud prevention.

[8] Contact Babel: US Contact Centers 2024-2028

Pindrop®

Schedule a call with one of our experts today

pindrop.com | info@pindrop.com