Ring's fraud team saves millions by shutting the door on returns abuse

Losses prevented in seven months

$4M+

Meet Ring

Since its founding in 2013, Ring has been on a mission to make neighborhoods safer for everyone. From the video doorbell to the award-winning DIY ring alarm system, Ring's smart home security product line and Neighbors app offer customers affordable whole-home and neighborhood security. An Amazon company, Ring is committed to making security accessible and convenient for everyone while working hard to bring communities together.

> "We prioritize customer satisfaction above all, so we have had to balance that against stopping policy abuse. But with Riskified, we can now selectively prevent abuse while maintaining attractive policies and a positive experience for our good customers."

Ramiro Rodriguez
Manager of Fraud & Risk Operations

The challenge

Ring offers both security hardware and subscription services to its customers. Like other digital retailers, it faces a dilemma when it comes to returns policies. Ring wanted to provide the generous policies consumers prefer, but knew those policies could invite abuse from bad actors.

For years, Ring erred on the side of generosity when it came to hardware returns. But when the fraud team began to see refunds rising, they suspected they had a problem with returns abuse. They partnered with Riskified in 2023 to take a closer look.

Together, they discovered a significant, organized pattern of abuse perpetrated by a relatively small number of individuals. Scammers would buy dozens of doorbells or other hardware items at once, file a return on the order, and return an empty box or box of junk. Scammers then collected a refund and were able to easily resell the popular items online.

Ring's fraud team knew they couldn't simply block bulk orders because not all high-value purchases were abusive. As a result, fraudsters were making thousands of dollars and creating pure losses for Ring, which was essentially giving away inventory plus paying two-way courier costs.

Riskified's assessment revealed that Ring was not only losing millions of dollars annually due to returns abuse, it was also prominently featured on dark web fraud sites as a vulnerable retailer.

The solution

With its automated tools and vast data intelligence, Riskified was able to gain clarity into the thousands of cookies, emails, and phone numbers scammers were using to obscure their identities and commit wide-scale fraud at Ring's expense. The analysis determined that just 600 individuals were responsible for $4M+ in abuse each year, with some committing as much as $150K annually.

Riskified's Policy Protect automation with Identity Explore technology gave Ring real-time insight that empowered the team to decline orders at checkout that would have led to fraudulent returns. The fraud team began with a conservative approach by manually reviewing declined purchases to be sure no legitimate customers were being turned away. But Ring soon confirmed that Riskified's decisioning was accurate and requested more aggressive declines.

In just seven months, Ring's fraud team was able to decline $4M+ in abusive returns that would otherwise have represented pure loss.

The results

Bottom-line savings

$4M

Abusive purchases
blocked in seven months

Identifying bad actors

600

abusers identified

> "Working with Riskified to stop these losses has increased our revenue retention dramatically, providing excellent ROI for us. The integration required was seamless and met our very rigorous requirements for customer data protection. It has been a win for the organization across the board."

Ramiro Rodriguez
Manager of Fraud & Risk Operations