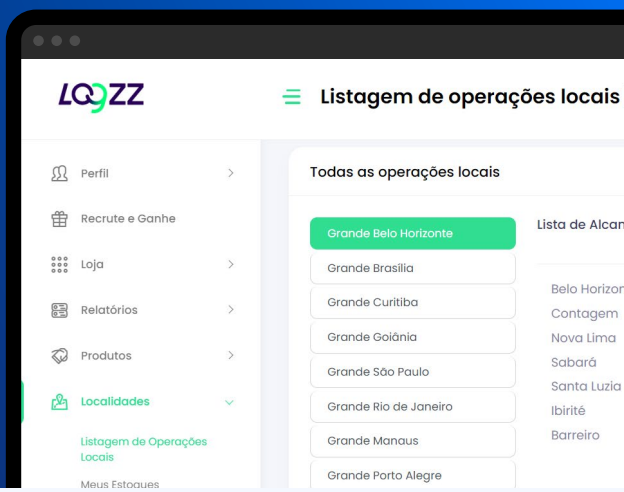
SHIELD | LOGZZ

Case Study

Logzz & SHIELD: Eliminating Fraud and Reducing Chargebacks in the Cash on Delivery Marketplace



"Our mission is to empower entrepreneurs to grow their businesses with greater confidence. With SHIELD, we're able to identify threats before they reach our users and protect our community from the very first click all the way through to cash in hand."

Rafael Munhoz
CEO & Founder, Logzz

Key Takeaways

92% decrease in chargeback rates

Millions of purchases protected

97% reduction in devices linked to fake accounts

Driving Secure Sales with the COD Model

Logzz has become the go-to marketplace for digital entrepreneurs, driving high conversion rates with its "cash on delivery" model. Consumers can place orders online and pay only upon delivery, avoiding the need to share sensitive information such as credit card details on the platform.

While this approach offers greater security for customers who prefer not to share their data online, the platform's rapid growth brought new challenges: fake account creation, fraudulent purchases, and a rising volume of chargebacks.

To safeguard its ecosystem, maintain the trust of producers and ensure that every sale reaches a legitimate buyer, Logzz partnered with SHIELD, adopting its Device Intelligence solution to detect risk in real time before approving any transaction.

Customer Profile
Founded in 2022, Logzz is Brazil's first digital platform operating on a "Cash on Delivery" (COD) model. It provides an ecosystem that connects producers, affiliates, and couriers to streamline the sale and delivery of physical products. With over 4,000 items listed, the platform has completed around 2 million deliveries across more than 200 cities in Brazil.

Industry
Marketplace

Region
LATAM

The Challenge: Large-Scale Fake Accounts and Chargebacks

As Logzz grew, the marketplace became an attractive target for fraudsters. The biggest risk came from the mass creation of fake accounts, which led to fraudulent orders, rising chargeback volumes, and eroded trust in the platform among producers and affiliates.

To carry out these attacks, fraudsters relied on bots and malicious tools capable of rapidly creating dozens of accounts while masking their identities. Common techniques included:

- **Proxies and VPNs**, which hid the real IP address and simulated logins from different regions;
- **Emulators**, which replicated multiple devices and confused device-based security measures;
- **Anti-fingerprinting tools**, which altered browser fingerprints to make multiple accounts appear as if they belonged to different users.

Once created, these fake accounts were used to exploit promotions and new-user coupons, as well as to place orders that would never be paid or would be paid with stolen cards, generating high logistical costs and an increase in cancellations.

The impact was significant: recurring chargebacks, direct financial losses, and declining trust across the ecosystem, ultimately compromising the experience for both producers and affiliates.

Device-First Fraud Intelligence for a Secure Marketplace

To protect its marketplace from large-scale fraud, Logzz integrated SHIELD's device-first fraud intelligence, designed to stop fraud at its root: the fraudster's device.

With SHIELD's persistent Device ID, the Logzz team can identify when a single device is linked to multiple accounts. In these cases, new logins are automatically blocked, preventing fraudulent purchases before they cause any damage.

Additionally, SHIELD's real-time Fraud Intelligence exposes advanced fraud tactics and malicious tools, such as emulators, proxies, and anti-fingerprinting solutions, used by fraudsters to disguise their activity and mimic legitimate users.

By embedding SHIELD into its ecosystem, Logzz eliminated large-scale fake account creation and fraudulent purchase attempts, restoring trust among producers and affiliates. They can now sell their products with confidence, knowing they are reaching real buyers with genuine purchase intent.