SumUp Reduces Chargebacks and Recovers Over R$ 420K with Axur's Preventive Monitoring

About the company

SumUp is a global fintech founded in 2012 that provides payment solutions and financial services for small and midsize businesses. Operating in 34 countries, it serves more than 3.5 million customers, expanding access to payment technology and supporting entrepreneurship.

Problem

In 2020, cybercriminals were successfully carrying out a high volume of checker attacks, fraud schemes that used SSN generators to create fake customer accounts. Fraudsters coordinated through Deep & Dark Web forums and groups to share tactics, exchange information about vulnerabilities, and organize attacks targeting SumUp customers.
Without visibility into these conversations, the company could only respond after chargebacks had already occurred.

Solution

Axur became a strategic partner in helping SumUp regain control over fraud impacting its operations.

Through continuous monitoring of the forums and groups where fraudsters were organizing, SumUp was able to map fraud schemes, understand attacker modus operandi, and block new attempts before they resulted in chargebacks.

Impact on operation

Over R$ 420K recovered in just 6 months

Positive ROI

Significant reduction in checker-driven fraud and fake registrations

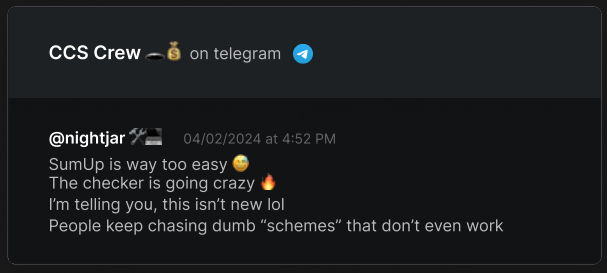


Image 1: Screenshots of fraudsters discussing SumUp before the partnership with Axur

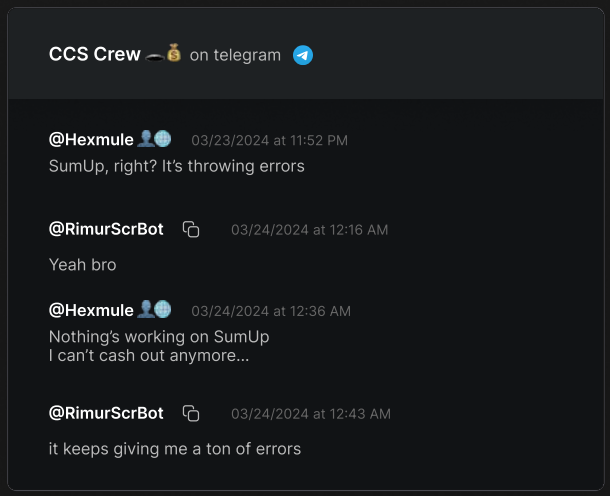


Image 2: Fraudsters complaining that it became virtually impossible to carry out scams on SumUp after the partnership with Axur

Solutions to Detect Threats Across the Deep & Dark Web

Proactively anticipating threats with cyber threat intelligence

Preventive monitoring of the Deep & Dark Web makes it possible to intercept conversations and identify active fraud schemes. Axur's platform tracks brand mentions, discussions about vulnerabilities, the sharing of customer data, and even the sale of compromised credentials.

This proactive approach replaces the traditional reactive model—where threats are only discovered after chargebacks have been filed and financial losses have already occurred.

Multimedia detection powered by computer vision

Fraudsters don't rely solely on text. They often share screenshots, tutorial videos, and images containing instructions on how to carry out scams.

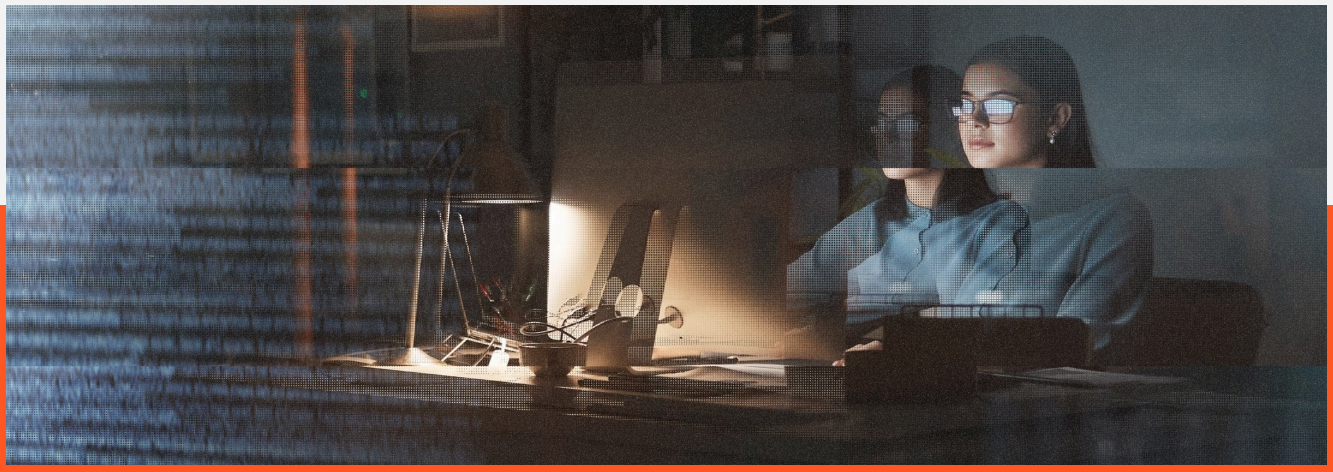
Axur's Computer Vision technology (Clair) automatically analyzes audio, video, and images shared on the Deep & Dark Web, transcribing content and identifying brand mentions even when the name appears only in visual form.

Investigation capabilities and customized alerts

The platform enables security teams to search and investigate any term related to their operation in a secure environment. In addition, custom alerts notify the team immediately when a new threat is detected, enabling a fast and coordinated response.

Fraud prevention impact

Axur's solutions help companies regain control of their brand, generate direct financial returns, and become essential for fraud prevention—especially during periods such as new product launches.



Learn how to protect your business from Deep & Dark Web threats

BOOK A DEMO

Gartner Peer Insights 4.9

Discover all our solutions: **axur.com**

///AXUR