Understanding fraud in e-Commerce

As e-Commerce businesses strive to provide seamless experiences for customers, fraudsters continuously seek vulnerabilities to exploit. To navigate this challenge effectively, it's crucial to understand the various forms of fraud that can threaten your operations.

Not every platform is the same, but across the board, e- Commerce businesses should take steps to address these leading types of fraud:

Social engineering fraud

The most common types of fraud attacks against e-merchants in 2022 were through social engineering tactics like phishing, pharming, and whaling[1]—designed to get individuals to reveal personal information like passwords and credit card numbers. Reseller bots, which are designed to buy items faster than a human can (so a fraudster can resell those items at a profit) were also prevalent.[2] In fact, 47% of online traffic in 2022 came from bots, and 20% of that bot traffic went on to retail sites.[3]

Account takeovers (ATO)

This is a form of identity theft where account access is compromised, and someone who is not the legitimate owner of the account takes control of the account. Account takeover losses increased by 90% in 2021[5], and 1/3 of all login attempts on retail e-Commerce sites were account takeover attempts.[6]

Communications fraud

Referred to as toll fraud, SMS pumping, or International Revenue Share Fraud (IRSF), this type of fraud is unknown by many businesses. It involves fraudsters that exploit vulnerabilities in SMS messaging systems used by e-Commerce businesses to trick the business into sending messages to premium rate numbers—generating a large volume of traffic and fraudulent charges to the business. This type of fraud costs businesses more than $8B annually, and an average attack can result in $50K in damages.[9]

New account fraud and fake accounts

Fraudsters attempt to create new accounts that aren't for real people—and they use bots to create them at scale when verification methods aren't in place. Once they're in, the types of potential fraud attacks are endless, from card testing and web scraping to inventory abuse and fake reviews that diminish seller credibility. Fraud from automated attacks was up 71% in 2022.[4]

Promo abuse

This is when fraudsters create multiple fake accounts to take advantage of discount codes, rewards, sales, and other types of promotions. Research suggests that $1B in rewards value is lost every year to fraud[7], and the promo abuse total for U.S. businesses in 2022 was $189B.[8]

Chargeback fraud

This type of fraud occurs when a customer intentionally disputes a charge, with the goal of receiving a refund, and keeps the product. 46% of merchants said that reducing fraud-related chargebacks was a top priority in 2022.[1]

Ready to delve deeper into strategies for combating fraud and reducing friction in e-Commerce?

Tap into the latest fraud protection insights by downloading our white paper today.

Get the white paper

[1] Source: Global Fraud and Payments Report 2022, Cybersource.
[2] Source: Statista.
[3] Source: Security Magazine.
[4] Source: The State of Fraud 2023, Signifyd.
[5] Source: Security.org.
[6] Source: Forbes.com.
[7] Source: Shopify.com.
[8] Source: Ekata/MasterCard.
[9] Source: 2021 State of Communications Fraud, Technology Research Institute.

Telesign provides Continuous Trust™ to leading global enterprises by connecting, protecting, and defending their digital identities. Telesign verifies over five billion unique phone numbers a month, representing half of the world's mobile users, and provides insights into the remaining billions. The company's powerful machine learning and extensive data science deliver identity risk recommendations with a unique combination of speed, accuracy, and global reach. Telesign solutions provide fraud protection, secure communications, and enable the digital economy by helping companies and customers to engage with confidence.