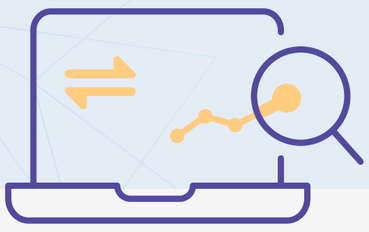
Arkose Labs

Q4 2019 Fraud & Abuse Report

Key Highlights



Arkose Labs analyzed over **1.3 billion** transactions across multiple use cases and industries

Overall attack rate **30%** higher

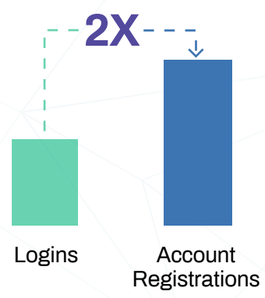
Over **1/2** the new account registration attacks on the technology industry are human-driven.

Account access (logins, reviews, updates) and account registration represent the bulk of the use cases, demonstrating the high engagement users have with their digital platforms.

70% higher bot-driven attacks for account registrations

Every **1/3** on financial services is human-driven with the most sophisticated ones coming from lone fraudsters with access to stolen identity information and the latest tools.

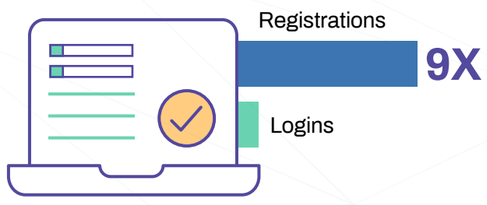
13.7% of all sessions are attacks. These attacks range from f**ake account registrations, promotion abuse, account takeover, inventory scraping, spam and fake listings.**



Account registration **attacks on gaming doubled**

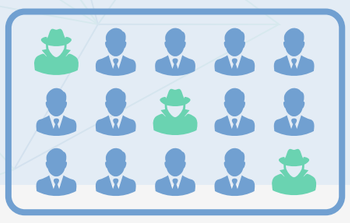
The attack motivations across the globe varies driven by **socio-economic differeces, access to technologiy and avaiability of cheap labor.** Arkose Labs' Attack Incentive Index provides insights into how the attack patterns vary from country to country.

An increase in attacks from malicious humans—both one off and organized fraud sweatshops. Nearly a third of all account registration transactions come from malicious humans.

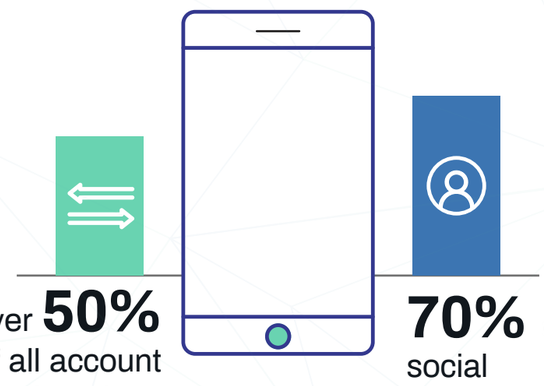


Tech registration is **9X** more likely to be attacked compared to logins

Arkose Labs is witnessing the emergence of **single request attacks** that mimic legitimate human users and can bypass traditional bot mitigation products.

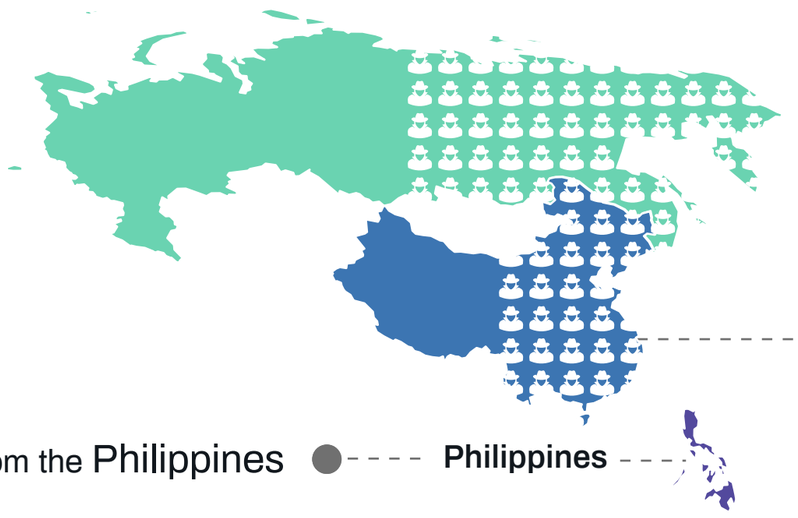


Nearly **1 in 5** of all account registration attacks are the most attacked customer touchpoint



Over **50%** of all account registrations are mobile-driven

70% of social transactions are mobile-based



Over half of the attacks from Russia and China are human-driven

60% decline in attacks from the Philippines

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Telemetry with an Adaptive Step-Up challenge. Telemetry accurately identifies bad actors, while the Adaptive Step-Up wears them down and diminishes their ROI without adding friction for good customers. The world's largest brands trust Arkose Labs to protect their customer journey while delivering an unrivaled customer experience.