Arkose Labs

6 HOTTEST FRAUD-FIGHTING TRENDS

DATA INSIGHTS FROM THE ARKOSE LABS GLOBAL NETWORK Q4 2021

What's Hot Right Now?

Top Fraud & Account Security Trends Across the Arkose Labs Global Network

Asia Attacks Proliferate

Nearly half of the attacks detected on the Arkose Labs Network last quarter emanated from China. This continues a trend of Asia being a major hotspot of both bot and low-cost human fraud farm attacks.

Rise of the Machines

Bot attacks have been steadily increasing throughout the year, with automation making up nearly 90% of all attacks in Q3. Expect this number to continue to hold steady and possibly even increase before the end of the year.

New Account Fraud Prevails

Fraudsters are creating fake accounts in droves across industries to monetize bonuses and go undetected within a platform. Q3 saw nearly 4x the volume of registration attacks as Q1 2021, contributing to almost ⅔ of attacks this quarter.

Credential Stuffing Spike

17% of all attacks during Q3 was a credential stuffing attack. This continues an ongoing trend as fraudsters aim to capitalize on the growth in digital accounts across the globe. Over the last 12 months, account compromises have nearly doubled compared to the previous 12 months.

Travel Fraud Resurgence

Attacks against travel companies were virtually nil during 2020, as pandemic-related lockdowns ground the industry to a halt. As planes refill with eager travelers, fraud targeting this industry has eagerly returned in kind, with attacks doubling compared to the first half of the year.

Holiday Fraud Heating Up

We're now entering the the biggest season for fraud -- the holiday shopping season. Attacks ramp up across all industries during this year, coinciding with a general spike in digital consumer traffic. During this holiday season, we anticipate upwards of 8 million attacks per day.

Crunching the Numbers: Key Quarterly Fraud Stats

Businesses are in a long-term, strategic battle against fraud. Arkose Labs monitors attack traffic across industries and geographies and reports on key statistics that indicate fraud trends which businesses all must be aware of. Overall, attacks have increased 15% compared to the previous quarter. Attacks on registration have nearly doubled in the last 90 days, and now is a top attack type. Ramping up to a busy holiday season, fraud has shifted more heavily to automation to help scale up attacks. As the holiday season quickly approaches, pay close attention to attacks across the digital front-end, and downstream monetization tactics.

Human vs Bots

12%
Humans

88%
Bots

Mobile vs Desktop

11%
Mobile

89%
Desktop

Global Attacks

17%
Attack Rate

15%
Rise in
Attack Volume

Top Attacked Touchpoints

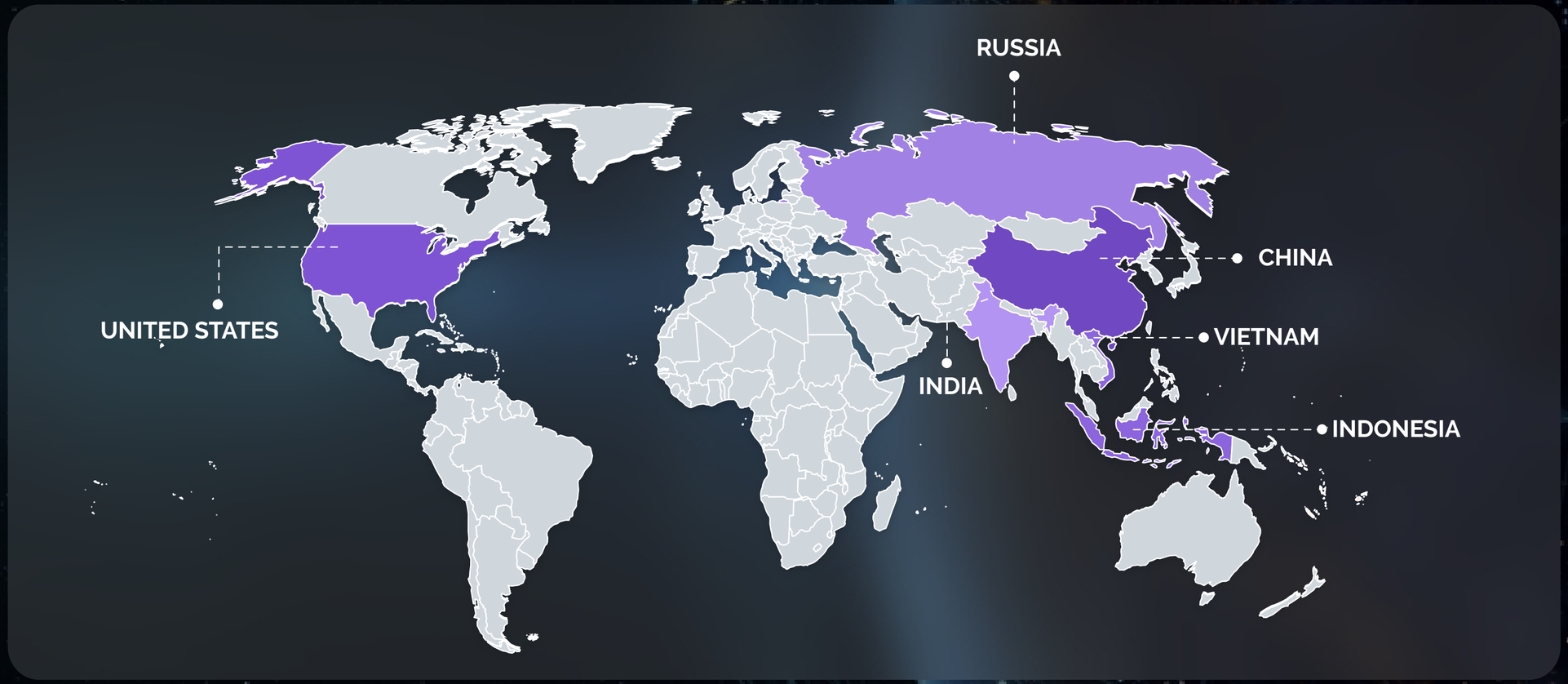
#1
Registration

#2
Login

Regional Trends: Asia Is The Leading Fraud Hotbed

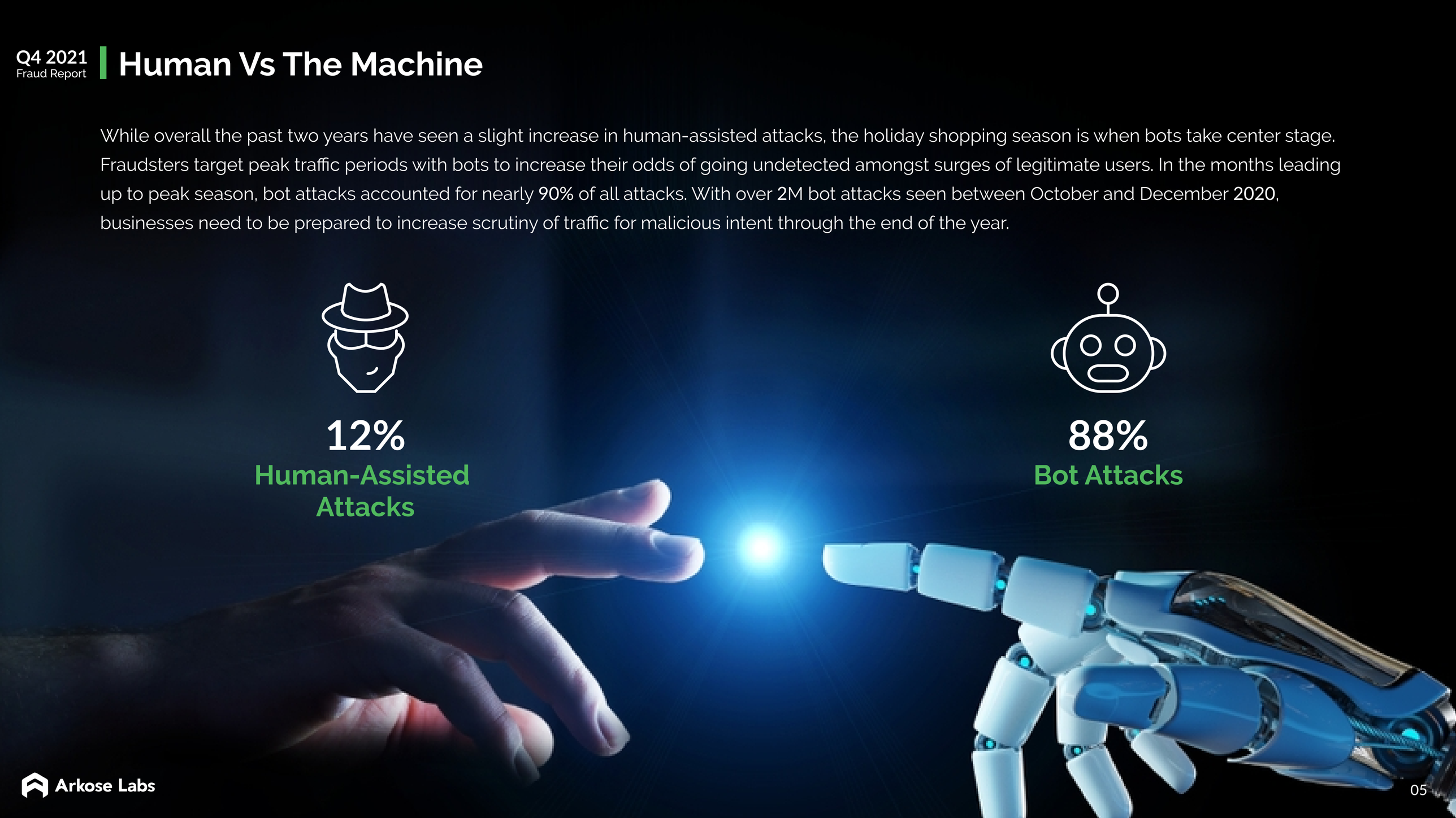
As 2021 has moved along, we have seen Asia return as the top geography where fraud attacks originate. The list of top attacking nations features China, Vietnam and Indonesia. Specifically, China in particular was a huge driver of attacks in Q3, being responsible for half of all attacks.

This was followed by the United States, with one-fifth of attacks originating from here. The other major attack hotspot was Russia, which has long been the major driver of attacks from the European region.



Human Vs The Machine

While overall the past two years have seen a slight increase in human-assisted attacks, the holiday shopping season is when bots take center stage. Fraudsters target peak traffic periods with bots to increase their odds of going undetected amongst surges of legitimate users. In the months leading up to peak season, bot attacks accounted for nearly 90% of all attacks. With over 2M bot attacks seen between October and December 2020, businesses need to be prepared to increase scrutiny of traffic for malicious intent through the end of the year.



12%
Human-Assisted Attacks

88%
Bot Attacks

Credential Stuffing Shows No Signs Of Slowing Down

One of the big reasons for the rise in bot attacks is to power credential stuffing attacks. In Q3 alone, Arkose Labs stopped over 140M attacks of this nature. More and more consumers are creating digital accounts for various reasons, which means there are more potential accounts to compromise. This is especially exacerbated during the holiday shopping season when consumers open more digital accounts. Bots are integral to this because they enable fraudsters to test thousands or even millions of different credential combinations in a short period of time.

5% of all digital traffic on the web is a credential stuffing attack

17% of all attacks were credential stuffing attacks last quarter

Credential stuffing attacks during the 2020 holiday season increased by 56%

3 billion credential stuffing attacks over the past year, nearly double over the previous **12** months

The Many Faces Of New Account Fraud

Account takeovers aren't the only use of stolen credentials. In 2021, digital businesses have seen a massive influx of fake new accounts disguised as legitimate users. In Q3 alone, the Arkose Labs Network detected 560M attacks on registration flows, nearly 4x the volume since the beginning of the year. These multifaceted attacks take many shapes due to the vast opportunities to profit off digital businesses. This includes securing sign-on bonuses, receiving funds without intention to payback, and spamming users with phishing attacks.

In a poll of 100 IT executives, 23% claimed fake accounts increased operational costs as they are typically a gateway to a multitude of spam and abuse.

Promo Abuse

Application Fraud

Account Validation Attacks

Synthetic Identity Farming

Affiliate Fraud

Spam & Abuse

Q3 Fraud Trends By Industry

Retail & Travel: Attacks Increased by 63% during Q3

Finance: 32% more attacks than during 1H 2021

Media & Streaming: 60% of attacks targeted the login point

Tech: 91% of attacks are powered by automation

Gaming: Registration most attacked touchpoint

Spotlight On: Fraud In The Travel Industry

As travel returned in the summer months, the travel industry saw a whopping **53%** attack rate in **Q3**. It comes as no surprise that digital traffic to travel sites rose a sharp **40%** in **Q3** over the previous quarter, sending this sector into high gear after being largely dormant for most of **2020** and early **2021**.

With this increase comes the rise in fraud targeting travel sites with large-scale bots and scraping attacks. While attacks in other industries originate from foreign nations, the vast majority of attacks on the travel industry came from the U.S, often driven by staunch competition in prices. There was also a huge shift to desktop-based attacks, which accounted for **85%** of all attacks targeting travel companies

53% attack rate in Q3 2021

85% of attacks are desktop-based

40% increase in traffic, driven by bots

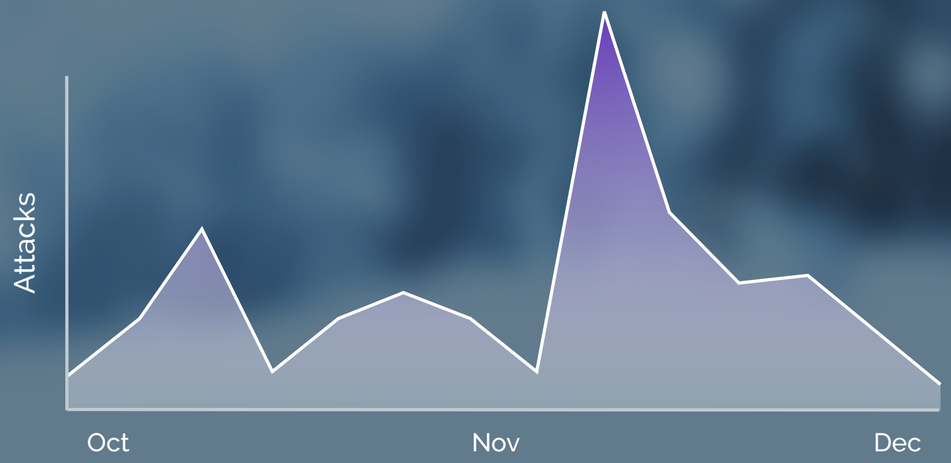
'Tis The Season For Holiday Fraud

Based on what we saw across the Arkose Labs Network in 2020, we predict there could be upwards of a 50% increase in attacks for the 2021 holiday shopping season. Credential stuffing is expected to be the main driver of these attacks.

Just like how the holidays are when many businesses make the bulk of their revenue, this is the time of year fraudsters launch attacks more frequently than any other time, taking advantage of the massive increase in digital traffic.

No industry will be spared, for example financial services, media, gaming and tech all saw a doubling of their average attack rate during holiday season 2020 compared to the prior quarter. In extreme cases, businesses will see a twenty-fold increase in attack volumes, which happened to one organization last year. This highlights the need for highly scalable fraud and security protections.

Up to 20x increase in attack volume in peak attack periods



Conclusion: Fraud Never Takes a Holiday

It is important to note that fraud does not have an off-season. The summer saw attacks continue to rise, and that trend will only increase as we get to the busy holiday shopping season. Year round, fraud attacks are becoming more frequent, launching on a greater scale, and increasing in profitability for those who initiate them. The tools and software that fraudsters rely on become cheaper to buy, easier to implement and more sophisticated. Thus, the shadow ecosystem that fraudsters depend on to carry out attacks efficiently and profitably becomes ever-more complex.

That's why businesses need a long-term fraud deterrence system in place that can detect attacks and stop them in real-time before they harm you or your customer. Companies need a solution that frustrates fraudsters to the point that they don't merely switch tactics and try again, but give up attacking your business entirely. Only then can you be assured to be free of fraud year round.

Arkose Labs

About the Arkose Labs Fraud & Abuse Report: The data in this report is derived from analysis across the Arkose Labs Global Network, which analyzes billions of transactions -- suspicious and non-suspicious -- around the world from multiple different industries. The Arkose Global Network allows all customers to benefit from anonymized shared intelligence. Historical attack pattern calibration correlates data across use cases and industries to detect anomalous activity and emerging attack patterns.

Offices

San Francisco
250 Montgomery St 10th Floor,
San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

Schedule Demo

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput. Based in San Francisco, CA with offices in Brisbane, Australia and London, UK, the company was honored as the 195th fastest growing companies in the United States on the 2021 Inc. 5000 list.