Arkose Labs

Brokering Trust in Online Marketplaces

P2P Marketplaces vs the Fraud Ecosystem

Ebook

The P2P Digital Revolution

When we talk of 'digital disruption', no phenomenon embodies this more than the rise of the sharing economy. The rise of peer-to-peer (P2P) online platforms, connecting individuals for direct commercial transactions, has exploded in the last decade.

It is an 'industry' that transcends traditional definitions, spanning retail, finance, lending, travel, transport, automotive, and more. The commonality of these businesses is that they offer dynamic platforms, connecting a decentralized pool of consumers and suppliers for better deals on goods and services.

This group of highly specialized businesses and start-ups are using technology to create brand new markets. Yet their success largely depends on its reputation as a secure space, giving individuals the confidence to transact with strangers without being scammed or defrauded.

Security is, therefore, a strategic imperative for businesses participating in the sharing economy. Due to their unorthodox business model, there is a unique flavor to their fraud prevention efforts.

A Day in the Life of a P2P Digital Native

The sharing economy has permeated into all parts of our daily lives, revolutionizing how we both spend and make our money.

In the United States alone, the number of adults using popular sharing economy services is forecast to grow to 86.5 million by 2021.[1]

Individuals have new ways to connect to distributed pockets of buyers and sellers. This has brought major disruption to established industries, including finance, transport, tourism and retail. The gig economy has flourished, as people embrace non-traditional ways of providing and accessing services and products.

Travel to work
in car share
TRANSPORT

Hire graphic designer
for a project
WORK

Buy new outfit
on marketplace
RETAIL

Book weekend away
HOLIDAY RENTAL

Connect with a new person
DATING

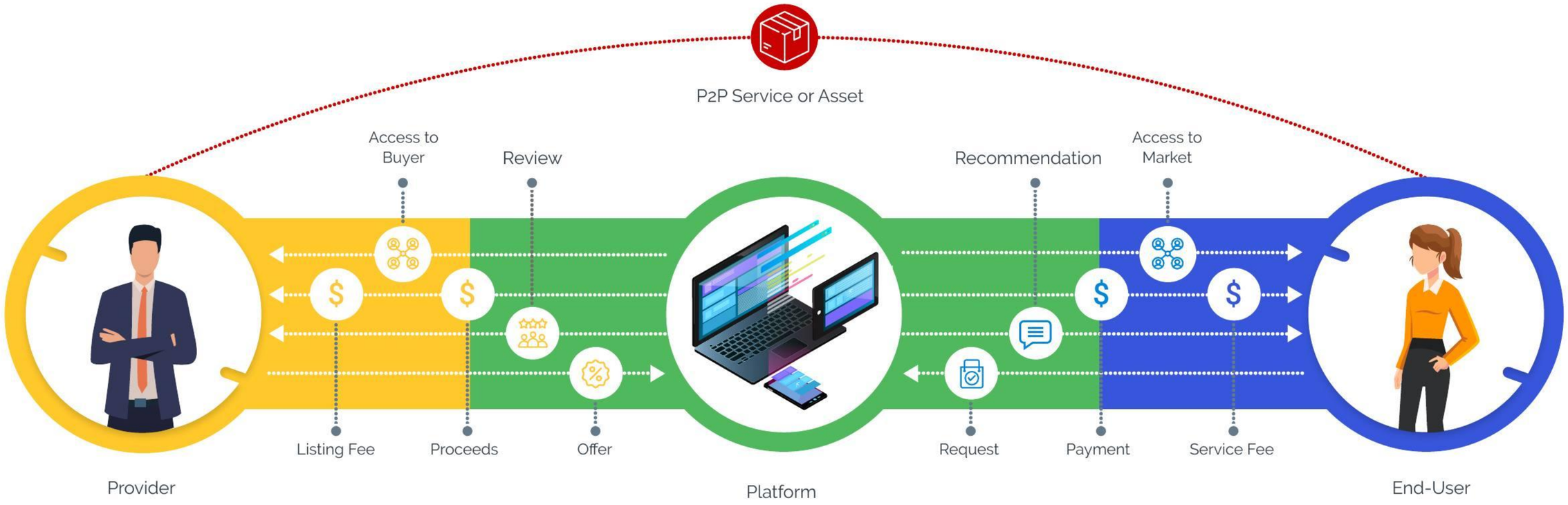
Apply for a P2P loan
LENDING

Bid to purchase
a car in auction
AUTO

[1] *https://www.statista.com/statistics/289856/number-sharing-economy-users-us/*

A Unique Business Model

P2P platforms and marketplaces operate a two-way business model which facilitates exchanges between third parties looking to access a decentralized network of providers and consumers. These platforms are the conduit for a range of interactions and financial transactions, depending on the exact service they are providing.



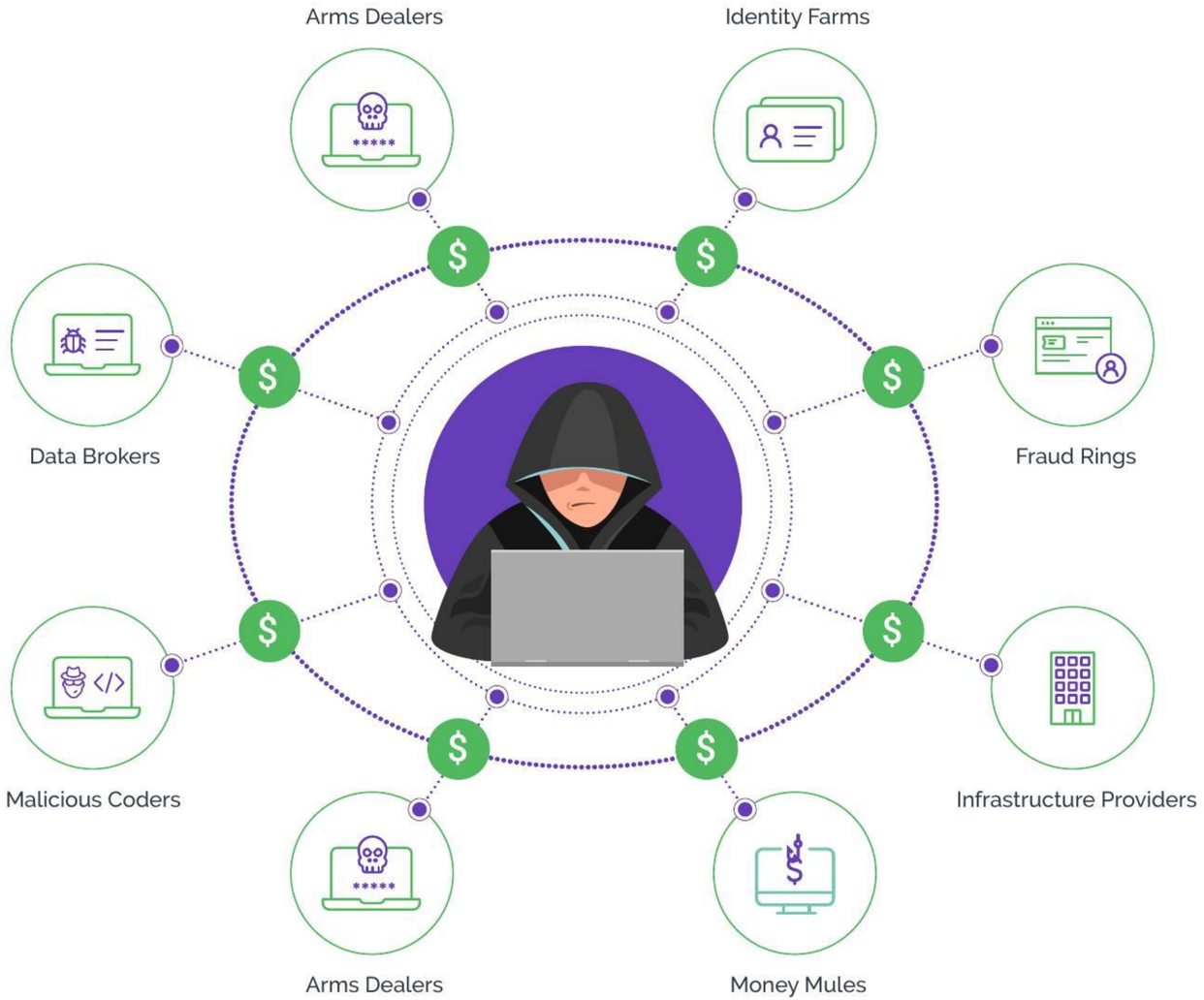
The Shadow Marketplace of Organized Fraud

The challenge facing businesses in the sharing economy is that they are coming up against a complex shadow cybercrime marketplace.

This multifaceted ecosystem has sprung up to support the 'business' of fraud, providing support services ranging from identity farms, malicious programmers, human sweatshops and money mules.

Fraudsters can tap into global resources and crowdsource information about the latest tools and techniques which are effective in bypassing businesses' evolving security controls.

This scattered network of services and information- sharing makes large-scale, organized fraud possible.



Trust is the Central Component of P2P Platforms

Online marketplaces and businesses in the sharing economy are not providing a tangible product or asset in the way traditional businesses do. They are facilitating connections between different individuals and third parties, and their core value is to provide a trusted intermediary platform.

The two-fold role of businesses in the sharing economy:

Technology platform with functionality that allows third parties to connect, communicate and transact.

Security and authentication capabilities which ensure the platform is a safe place to transact with unknown users.

Mimicking Trust is the Core Business of Fraud Marketplaces

The shadow cybercrime ecosystem provides tools and resources for fraudsters to masquerade as legitimate users and circumnavigate advanced fraud prevention controls. A truly lone operator would struggle to consistently drive profit from fraud when coming up against a mature fraud prevention team and its technological defenses. However, when fraudsters tap into the data, tools and knowledge of a cybercrime network, it makes it increasingly difficult for businesses to differentiate between trusted and malicious traffic.

Pass authentication using human sweatshops

Spoof identity using stolen and synthetic credentials

Obfuscate true identifiers to launch single request attacks

Mimic trusted devices

Hide true location

Imitate trusted behavioral patterns

High-velocity identity testing using bots

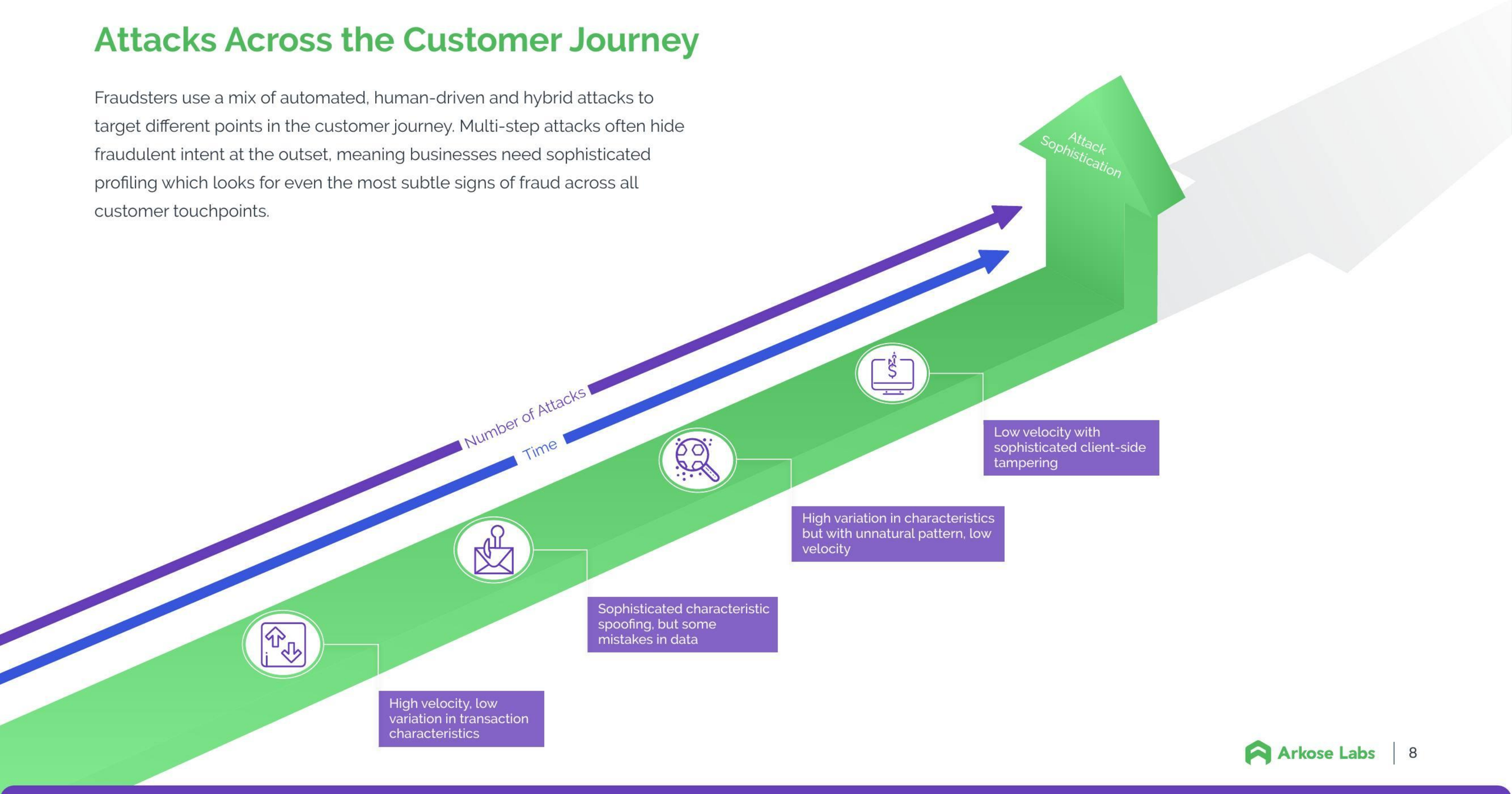
Securing the Customer Journey

Fraud departments need many strings in their bows, with effective fraud prevention plugged into every step of the dual user journey - protecting both buyers and sellers on both sides of the platform.

Companies in this fast-growth sector need to identify fraud prevention technologies that are highly effective across multiple fraud and abuse use cases. This way they can scale rapidly and securely, without being slowed down by a complex technology stack which places a significant burden on in-house resources.

Attacks Across the Customer Journey

Fraudsters use a mix of automated, human-driven and hybrid attacks to target different points in the customer journey. Multi-step attacks often hide fraudulent intent at the outset, meaning businesses need sophisticated profiling which looks for even the most subtle signs of fraud across all customer touchpoints.



Four Key Pillars of Fraud Prevention in the Sharing Economy

The major challenge comes in orchestrating multi-layer fraud prevention across all customer touchpoints, on both sides of a P2P platform or marketplace, without getting bogged down by complexity.

As this innovative industry continues its rapid growth, it is becoming a bigger target for fraudsters. However, digital-savvy users have very little tolerance for security controls which slow them down or restrict access to the shared marketplace.

What are the strategies businesses can put in place to navigate an increasingly hostile threat landscape, while reducing complexity and enhancing the user experience?

1 Unified Protection Across Use Cases

While there will never be a single silver bullet that solves all fraud and abuse issues, a crucial part of long-term success is to prioritize investments based on versatility across use cases, as well as efficacy as a point solution.

Fraud departments in the sharing economy potentially have twice the number of touchpoints to protect due to its dual business model. To protect against more complex fraud patterns using multi-step attacks, they need a unified view of risk across the full customer journey.

By deploying fraud prevention technologies that can detect different forms of abuse, across various customer touchpoints, businesses can improve their security without over-complicating their fraud technology stack.

BENEFITS OF UNIFIED RAUD PREVENTION

- Shared fraud data across touchpoints
- Multi-step attacks easier to detect
- Simpler fraud technology stack
- Lower operational costs
- Unified view of risk

BENEFITS OF AN INTERMEDIARY PLATFORM FOR FRAUD AND ABUSE PREVENTION

- Disrupts fraudsters' attack techniques
- Lightens the burden on in-house teams
- Crowdsources threat intelligence
- Independently analyzes traffic
- Simplifies workflow across use cases

2 Shift the Attack Surface

Fraudsters rely on tried and tested ways of attacking websites and apps directly, and evolve these tactics as fraud prevention methods advance. Industries find themselves in a perpetual cat and mouse game trying to stamp out large-scale fraud, with the strain on in-house teams increasing despite increased investments in fraud prevention capabilities.

Diverting suspicious traffic to an intermediary platform, which delivers risk profiling and tailored authentication challenges, can serve as a highly effective buffer between the business and the attacker. Not only does this relieve the burden on internal talent, it is a powerful way to claw back control from organized fraud by disrupting perpetrators' modus operandi.

Businesses in the sharing economy who are looking for the most streamlined fraud operations need to identify trusted partners to provide independent verification of traffic hitting their sites, so they can operate in confidence that the transactions that make it through to them are legitimate.

3 Strategic Use of Friction

Good users' behavioral patterns are evolving, and fraudsters are able to mimic legitimate consumer activity more effectively than ever before due to sophisticated tools and vast swathes of stolen identity data. Fraud systems which rely purely on risk-based analysis are finding more and more traffic is falling in the gray area between 'good' and 'bad' activity.

The concept of "friction" has become undesirable due to the negative impact on customer conversion rates from legacy solutions. However, when friction is directed specifically at risker traffic, this is a highly effective dual approach which validates risk-based data insights using intelligent step-up authentication.

Fraudsters will quickly become disengaged when they meet increased resistance as it takes additional time, effort and resources to complete the authentication steps. This is a smarter way to improve the security and user experience for good customers.

BENEFITS OF A TARGETED FRICTION

- Unified risk-based and step-up authentication
- Protects good user experience
- Reduces "gray area" traffic
- Cuts fraud losses

BENEFITS OF A STRATEGY CENTERED ON ECONOMIC DRIVERS

- Long-term protection against evolving fraud patterns
- Reduce spiraling fraud prevention costs
- Relieve burden on in-house teams
- Cut fraud losses

4 Break the Fraudsters' Economics

Many organizations see the fight against fraud as a technology arms race. However, this mentality often leads to growing fraud budgets - despite fraud rates still being on the ascent.

For more nimble companies in the sharing economy, there is an opportunity to adopt an entirely different attitude to fraud prevention.

Rather than viewing fraud prevention purely as a technology issue, many organizations are coming to see it as a strategic battle rooted in economics. While there is money to be made on websites and apps, fraudsters will attack them. However, the minute the cost of attacks outweighs the potential profits, perpetrators will abandon attacks.

P2P companies need to identify and prioritize fraud defenses which drain perpetrators' time and resources for longer-term fraud prevention. Fraud tactics and techniques will evolve over time. Therefore, defenses will also have to stay dynamic and most importantly stay resilient against being scripted around en masse.

Global P2P eCommerce Marketplace

A global platform that connects buyers and sellers for direct e-commerce sales was being targeted with a sustained campaign of hybrid attacks using trained bots and human sweatshops. Fraudsters were posing as legitimate users in order to post fake listings to defraud buyers. They were hacking into good users' accounts to carry out payment fraud and post fake reviews of its bogus vendors. The company was relying purely on risk-based authentication. But, in the face of advanced attacks, which leveraged user credentials stolen in data breaches, there was an increasing volume of traffic that fell within the "gray area" between activity that was recognized as trusted or malicious.

Business Scenario

- Rising fraud losses
- High manual review rates
- Growing demands for fraud personnel and budget
- Lack of visibility into trustworthiness of reviews

Solution

- Combined risk-based and step-up authentication
- Risk-based profiling to authenticate trusted customers
- Incrementally complex step-up challenges directed at suspicious traffic

Results

- Dramatic uptick in the number of automated attacks blocked
- Identified and stopped sustained attack from organized fraud ring
- Stable good customer throughput rates

Zero Tolerance Approach to Fraud and Abuse on P2P Platforms

To stop all automated attacks and slow fraudsters down to the point that attacks become economically non-viable, businesses need a holistic approach that spans both risk-based and step-up authentication.

1. Detect suspicious traffic using multi-layered risk profiling.

2. Triage traffic according to its risk profile for tailored authentication workflows.

3. Use targeted friction to eliminate all automated attacks.

4. Deploy graduated challenges which root out sweatshop activity.

5. Feed results of step-up challenges into the risk-based profiling. for continuous refinement.

Arkose Detect is Trained by Arkose Enforce Results

Arkose Labs' Fraud and Abuse Prevention Platform provides an innovative, streamlined approach by combining risk-based decisioning and targeted enforcement challenges in one plug-and-play solution.

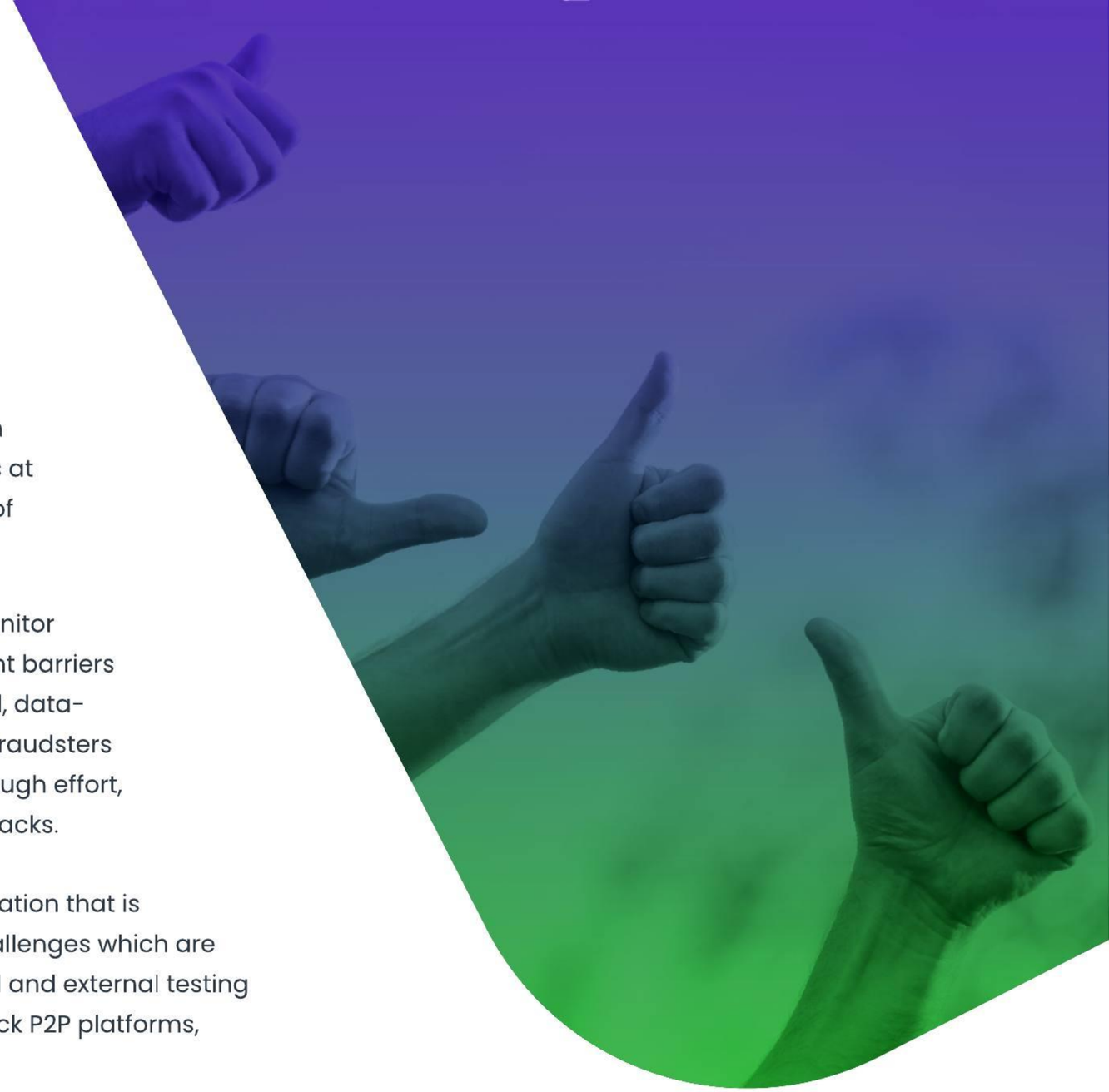
Brokering Trust

Stamping out fraud and abuse is absolutely central to the success of P2P platforms and marketplaces. The minute that users stop trusting that a platform is brokering introductions to legitimate individuals with good intent, the business model falls apart.

However, businesses are facing a multi-faceted cybercrime network, which provides a host of support functions to fraudsters looking to launch attacks at scale. Due to the dynamic nature of the sharing economy sector, the type of fraud companies are facing is evolving rapidly.

For a long-term protection against attacks, fraud departments need to monitor activity in a way that is non-intrusive for true users, while providing sufficient barriers to risky traffic in order to disincentivize fraudsters. Combining sophisticated, data-driven fraud detection with targeted friction roots out automated attacks, fraudsters and sweatshops. The downfall of many legacy approaches is that with enough effort, fraudsters will script round defenses and launch low-cost, high-volume attacks.

For this reason, companies need a more creative approach, with authentication that is constantly evolving by design. Presenting risky traffic with enforcement challenges which are resilient to being solved by machines - and checked thoroughly by internal and external testing techniques - will sap the time and resources required by fraudsters to attack P2P platforms, compelling them to abandon attacks and move on.



About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319
arkoselabs.com

Offices

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

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo