Arkose Labs

2022 FRAUD & ABUSE PLAYBOOK

Top insights on how to navigate the changing fraud landscape.

- OUR CHANGING **WORLD**
- ACTION **PLANS**
- ARE BUSINESSES **PREPARED?**
- 2022 FRAUD **MANIFESTO**

A MANIFESTO FOR STOPPING FRAUD

> AS AN OLD SAYING GOES...
> "There are decades where nothing happens; and there are weeks where decades happen."

Throughout 2021, the world began to recover and our lives started to appear more and more like pre-pandemic era. However, there are some aspects of our society that are forever changed. Due to the pandemic, businesses had to adapt to unique circumstances and evolve to suit an online environment. As businesses made changes, fraud followed like a moth to a flame.

Projections for 2022 and beyond show it is clear that without urgent action, fraud will evolve to be faster and more efficient, becoming more profitable than ever. To stem the rising tide, your business needs to take a zero-tolerance approach that addresses the root causes of fraud. This requires a clear understanding of the financial incentives and implications of attacks. Fraudsters have easy access to a complex ecosystem of tools and people to help them commit attacks at scale while maximizing profit.

The nature of attacks is constantly changing, with fraudsters becoming increasingly creative in their approach. To combat this, internal fraud and security teams must be equally innovative, and view fraud prevention strategy as an essential driver for long term growth.

Finally, all this must be done without impacting user experience. You can have the greatest fraud defenses in the world, but if it also stops your real customers from accessing your site, it is worthless. Balancing fraud prevention with user experience is a fine line that digital businesses must get right.

With that in mind, here is a five-point manifesto for successfully stopping fraud in 2022. In addition to our own expertise, this paper is based on insights from the 50+ speakers in the 2020 Bankrupting Fraud Summit, which was hosted by Arkose Labs at the end of 2020.

Arkose Labs

2022 FRAUD AND ABUSE MANIFESTO

THRIVING IN AN EVOLVING THREAT LANDSCAPE

1 UNDERSTAND THE CYBERCRIME ECOSYSTEM

Fraud is never created in a vacuum; each attack is the product of a highly interconnected critical ecosystem. Understanding how fraudsters utilize this ecosystem and undermining is the key to successfully stopping attacks from being carried out.

2 MONEY MATTERS

No one commits fraud just for fun. Attackers are highly motivated to make money, and drastically reducing the potential ROI they can make from attacks stops their ambition to launch them in the first place.

3 DEFEND AGAINST FULL RANGE OF ATTACKS

Fraud attacks can be accomplished using bots, humans or a mixture of both; and across a multitude of digital touchpoints. Understanding all the different attack types and the nuances behind each gives businesses the upper hand in identifying and preventing attacks on their platform and their customers.

4 CHAMPION THE CAUSE INTERNALLY

Fraud is not typically thought of as a strategic driver of business growth, but it should be. Successful businesses will put a strategic focus on fraud and security, realizing they are imperative to driving revenue and creating loyal customers.

5 PRIORITIZE UX

Fraud prevention is a balancing act between creating resistance that frustrates the bad guys' efforts and protecting a good user experience. User-centric security measures are the key to success - but beware approaches that are too lax, as they will spur on future attacks.

01

DEFENDING AGAINST THE INTERCONNECTED CYBERCRIME ECOSYSTEM

OUR CHANGING WORLD

Fraud is like any other job: people wake up each day and go to work to make money (virtually, like many of us in the post-COVID world). For fraudsters, the ROI for attacks must be worth it: they have to make more money than they spend on launching attacks.

Luckily for them, and unluckily for us, fraudsters have access to a global ecosystem that makes their attacks profitable. There is a comprehensive set of shadow services which enable individuals to tap into the resources required to carry out attacks at scale and learn off one anothers' successes.

The one constant in the fight against fraud is perpetual change. As a result of the interconnected cybercrime ecosystem, the techniques, tactics, and strategies used to commit fraud are always evolving. Attackers have a constant stream of fresh data and fresh tools with which to attack businesses. They are able to share successful attack techniques and are constantly iterating on one another's approaches.

HOW WELL ARE BUSINESSES PREPARED?

A consequence of the organized nature of fraud today, is that the touchpoints that are being attacked within businesses are profilterating, with attackers finding increasingly inventive ways to monetize abuse.

Companies need to improve their ability to spot and defend against attacks across the full spectrum of customer interactions. Beyond traditional fraud prevention, they need solutions that can work flexibly across both use cases and devices. They also need to be better prepared against the different attack types in the oponents' arsenal - ranging from low-sophistication, high velocity bots, to more nuanced human-driven or hybrid attacks.

ACCOUNT REGISTRATION

Fake Account Registration | Credential Testing | Bonus Abuse

ACCOUNT PROTECTION

Credential Stuffing | Account Takeover | Payments | Loyalty Points

SPAM & ABUSE

Inventory Hoarding | Scraping | In-Game Abuse | Fake Reviews | Spam

PROTECTING FULL CUSTOMER JOURNEY

DEKSTOP

CONSOLES & SMART TVS

MOBILE

ACTION PLAN

- Proactively examine all customer touchpoints to identify possible routes to monetization for fraudsters.
- Prioritize solutions that work across all the devices that consumers use to interact with you for a unified approach across channels.
- Build your defenses under the assumption that cheap, stolen data is being used at scale to attack using both automation and human "guns for hire".
- Play an active role in the anti-cybercrime ecosystem. All businesses need to collaborate closely via industry groups, consortium and vendor user groups to share key information.

02

HOW TO UNDERMINE THE BUSINESS MODEL OF FRAUD

OUR CHANGING WORLD

Fraud is a huge, multinational business that targets all sectors. It is powered by complex networks of highly skilled fraudsters, human fraud farms and malicious bots. This business must be viewed like any other: profit is the main motivator. The direct victims of fraud include businesses and their customers, but the wider consequences are more sinister. The proceeds of fraud act as a major funding stream for serious organized crime including the drug trade, human trafficking and major terrorist attacks.

Neil Walsh

CHIEF OF CYBERCRIME

UNITED NATIONS

"Fraudsters are generally not concerned with the threat of jail. It's merely an occupational hazard. They know it's going to happen at some point. But taking their money from them is what hits them the most. Criminality is profit-motivated; they're in it to make money and nothing else. They're not doing it for the good of their community. That's why breaking the economics of attacks is the single most effective way to stop fraud."

MONEY MOTIVATION

The low-cost, high-reward cybercrime ecosystem is based on several global socio-economic factors, which create different incentive levels for committing fraud. In regions with low costs of living and weak currencies, individuals stand to gain a great deal by attacking US businesses and will be willing to expend more effort on attacks, while still preserving ROI.

On top of the economic drivers, different regions across the globe have different access to the technology that is needed to support sustainable cybercrimes and launch large-scale fraud attacks. Countries with very low internet penetration rates are unlikely to become major fraud hubs.

The key to bankrupting fraud is understanding your adversary. The most successful fraudsters aren't necessarily good at coding or hacking, but rather excellent con men. They know which networks to tap into for resources and who to hire to help them carry out their attacks.

GLOBAL SOCIO-ECONOMIC FACTORS DRIVING FRAUD

Wages & cost of labor

Employment rates

Costs of living

Currency disparity

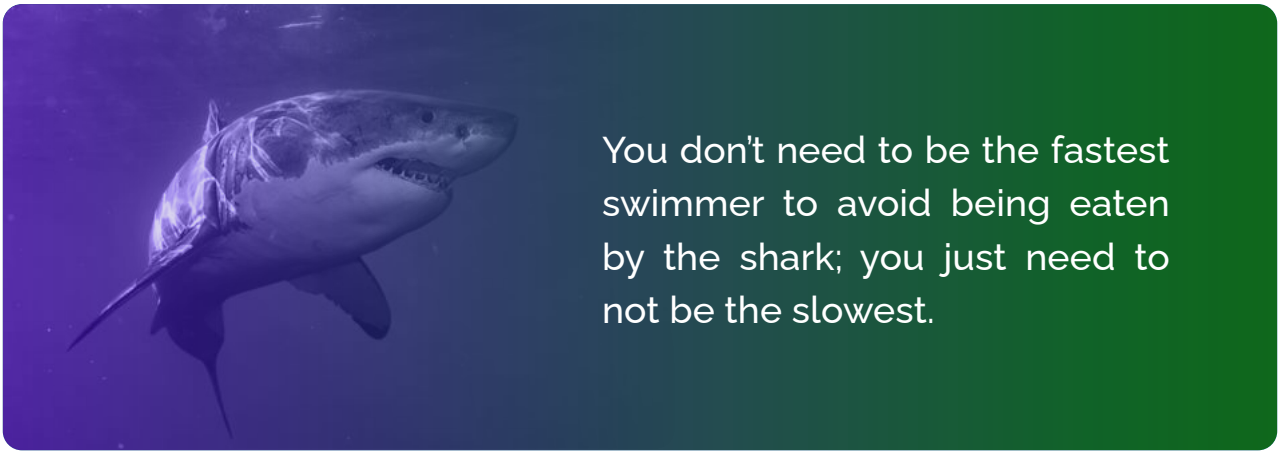
Access to technology

HOW WELL ARE BUSINESSES PREPARED?

The most foolproof way to stop fraud is remove the financial incentive. This means many businesses need to rethink their entire fraud prevention strategy. Current strategies are focused more on fraud mitigation, which ends up in a constant cat-and-mouse game between businesses and fraudsters. Go beyond a tactical, tool-driven view, and focus on the bigger picture. Long-term fraud prevention should work to achieve one simple goal: undermine the economic drivers behind fraud.

ACTION PLAN

- Keep the economic incentives behind attacks front and center when planning effective fraud prevention.
- Adopt tailored defenses to deal with the spectrum of high-volume, low-value attacks; versus more targeted and time-consuming, high return attacks.
- Prioritize fraud prevention measures that make it more costly to attack your site, compelling attackers to look elsewhere.
- Deploy highly targeted friction on suspicious traffic to frustrate fraudsters, without killing good user throughput.



03

UNDERSTAND THE LATEST FRAUD TRENDS

OUR CHANGING WORLD

Businesses have gone digital and with it, consumer habits have changed for good. As people are spending more time online than ever before, attackers have found new ways to exploit them. Here are 5 key takeaways on attack trends as digitization continues to expand.

1

With banking services now being available online, attackers have found ways to exploit security features and account confirmation processes. **Chargebacks and friendly fraud** attempts have rocketed since 2020. These account for 60-80% of digital fraud and range from innocent mistakes, where a consumer doesn't recognize a transaction to opportunism, where a consumer claims fraud where there is none.

2

New attack vectors opened as the demand in online shopping went through the roof causing a spike in **price gouging and non-delivery scams.** Attackers will post an item for sale that they never intend to deliver or hike up the price for stolen high-demand items. The stakes are high for fraud teams, as if they decline the wrong transaction, they prevent customers from receiving their goods.

3

Alongside the increasing popularity of online shopping comes the acceleration of digital payments. Financial services are seeing a rise in **card-not-present fraud** as the massive increase in digital payments becomes a lucrative target for fraudsters.

4

As more business is conducted online, more consumers are creating digital accounts. This has launched an opportunity for fraudsters to create **fake accounts** to spread **in-platform and phishing scams** by posing as the associated brand.

HOW WELL PREPARED IS YOUR BUSINESS?

To successfully defend against fraud, you need to know how fraudsters attack your particular industry. Attack types and goals differ depending on the target. It's important to understand how your business fits into the fraud ecosystem.

INDUSTRY	TARGET
RETAIL & TRAVEL Payment fraud, loyalty points, inventory hoarding, account takeover, scraping	Compromised consumer data leaves retailers' customer accounts vulnerable to credential stuffing and ATO attacks and the stealing of loyalty points, payment credentials and other personal information. Hosting business online is the new norm which increases the importance of account security. Now is the time for businesses to address security issues.
GAMING Digital currency, in-game items, valuable accounts, bonus abuse	The massive rise in new users means gaming companies often struggle to detect fraud amidst spiking traffic. Fraudsters take advantage of this by creating bot accounts at scale, which are then used to commit bonus abuse or manipulate in-game economies.
FINANCE/FINTECH Bank account information, payments data	Compromised financial accounts allow attackers to drain funds or commit a range of downstream fraud. While security is generally high in financial services, the rise of fintechs and challenger banks puts teams under increasing pressure to provide robust authentication, without forcing users out of band.
MEDIA/STREAMING Account log in information/ phishing messages to good users, spam	Streaming and media services are targeted for automated credential stuffing attacks; fraudsters then resell subscriptions. Social media, on the other hand, sees a wide range of attacks, including fake new accounts used to send phishing messages, information scraping, and the dissemination of false information.
TECHNOLOGY PLATFORMS Info scraping, spam/abuse, bonus abuse	Fraudsters target these platforms in a number of different ways, including creating fake accounts en masse to obtain free server time on software development platforms, and targeted ATO attacks on business networks in order to obtain valuable information, or to extort money. Some attacks aren't even financially motivated, that just aim to disrupt the user experience.

SPOTLIGHT ON ACCOUNT TAKEOVER FRAUD

There are currently more than 15 billion compromised account credentials available on the dark web, according to one study[1]. The potential downstream abuse from a successful account takeover is limitless: stealing personal or financial information; draining currency, loyalty points or other assets; fraudulent purchases, or using accounts to send malicious content and scams.

To effectively defend customers and businesses from account takeover attacks, it is important to understand the methodology and motivation of the attack. Attacks can be orchestrated by one individual or group, or form part of an identity farm's services.

HOW AN ATO ATTACK IS LAUNCHED

A successful attack has three major steps:

Credential Harvesting

The Fraudster collects a list of valid credentials. Techniques used to acquire or harvest them may vary dependng on the vertical

Credential Checking

This step is also referred as credential stuffing where the attacker is replaying the credentials list against multiple targeted websites

Account Takeover

A Fraudster will use bots or manual labor to login, take over the account and commit fraud.

ACTION PLAN

Checklist: Protect Your Business and Your Customers from ATOs

Protecting your business and your customers from ATOs

- Businesses must play their part by investing in strong network security and IAM to stem the leak of identity information and credentials.
- Ditch free solutions which are bypassed by bots and ensure all web forms are properly protected from automated credential testing.
- Monitor login attempts to digital accounts in real-time, classifying traffic into legitimate users, suspected bot, and human-driven fraud attempts.
- Use secondary screening to test high-risk traffic with authentication steps designed specifically for that threat type.

[1]*Winder, Davey "New Dark Web Audit Reveals 15 Billion Stolen Logins From 100,000 Breaches" Fprbes. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=5eceaec8180f*

04

ELEVATE THE STRATEGIC IMPORTANCE OF FRAUD & ABUSE PROTECTION

OUR CHANGING WORLD

Too often, fraud is seen as merely a cost center by executives and other decision makers. However, when properly deployed, fraud and security are key drivers of profit and essential in preserving a good brand image. The reality is that fraud prevention is critical to growing revenue and maintaining the bottom line.

HOW WELL ARE BUSINESSES PREPARED?

Businesses face the challenge of balancing growth and risk with fraud management. They have historically struggled to ensure a seamless customer onboarding experience, without offering fraudsters the same benefit. Increasingly fraud and risk teams are collaborating with product, marketing and strategy teams in pursuit of the same goals: successful growth, smart risk management, and robust fraud protection.

SUSTAINING GROWTH IN A POST-PANDEMIC WORLD

- **Know your customer:** An in-depth understanding of individual customers provides a powerful basis for identity verification.
- **Bring the benefits of bricks and mortar online:** A hybrid 'digital backed by people' approach provides customers with a streamlined, efficient service supported by real humans when necessary.
- **Communications is key:** Provide multiple options including phone, video messaging and online chat to best meet the needs of a diverse customer base.
- **Refine your product:** Competition is stiffer than ever, with businesses of all sizes scaling-up and benefiting from innovation. The product must be excellent, user-friendly, relevant to customers and the society they live in, and good for business.
- **One-stop shop:** Make it easy for customers to get the services they need in-house. Offer relevant partner products to help streamline operations.
- **Prioritize efficiency for consumers and the business:** This doesn't just drive down costs, but should be tailored to create user-friendly products that meet individual needs.
- **Invest in fraud prevention:** A proactive rather than reactive approach that integrates fraud prevention into all parts of the customer experience will safeguard profit and reputation.

ACTION PLAN

1

PROPERLY QUANTIFY THE ROI

Fraud departments need to start showing how successfully stopping attacks leads to revenue generation. For example, if a major bot attack was thwarted, what is the dollar value of money saved?

2

EMBED FRAUD PREVENTION INTO DIGITAL

Large teams are no longer required to be on-site, servers are monitored and even power switches turned on and off remotely. The pandemic accelerated the much-needed digital transformation of security programs.

3

STEM THE RISING TIDET

With fraudsters constantly recruiting and scaling up rapidly, businesses must realize the importance of investing in robust fraud and security departments.

4

FRAUD PREVENTION AS SALES DRIVER

Strong fraud and security protocols also support marketing and sales functions allowing these departments to demonstrate that safe user experience leads to happier customers, and enables new customer acquisition.

5

MOVE THE TARGET ELSEWHERE

Fraudsters regularly share information; if a particular site becomes known for having lax security controls in place, you can be sure that word will get around.

05

DELIVER EXCEPTIONAL UX FOR AN EXPANDED DIGITAL CUSTOMER BASE

OUR CHANGING WORLD

Given the drastic fluctuations in digital traffic levels and the severity and frequency of fraud attacks in 2021, it's highly likely this trend of constant change will continue. Many businesses were caught flat-footed after mass digitization led to a surge in fraud, and struggled to cope with this new reality. It really drove home the point that fraud and security teams can never rest on their laurels, and must always be prepared.

Digital traffic is only going to continue to spike and remain at increased levels -- it's been said that once humans adopt habits, they are difficult to reverse. Your business must be prepared to handle this increased usage while not affecting the digital experience, while at the same time remaining vigilant about stopping fraud.

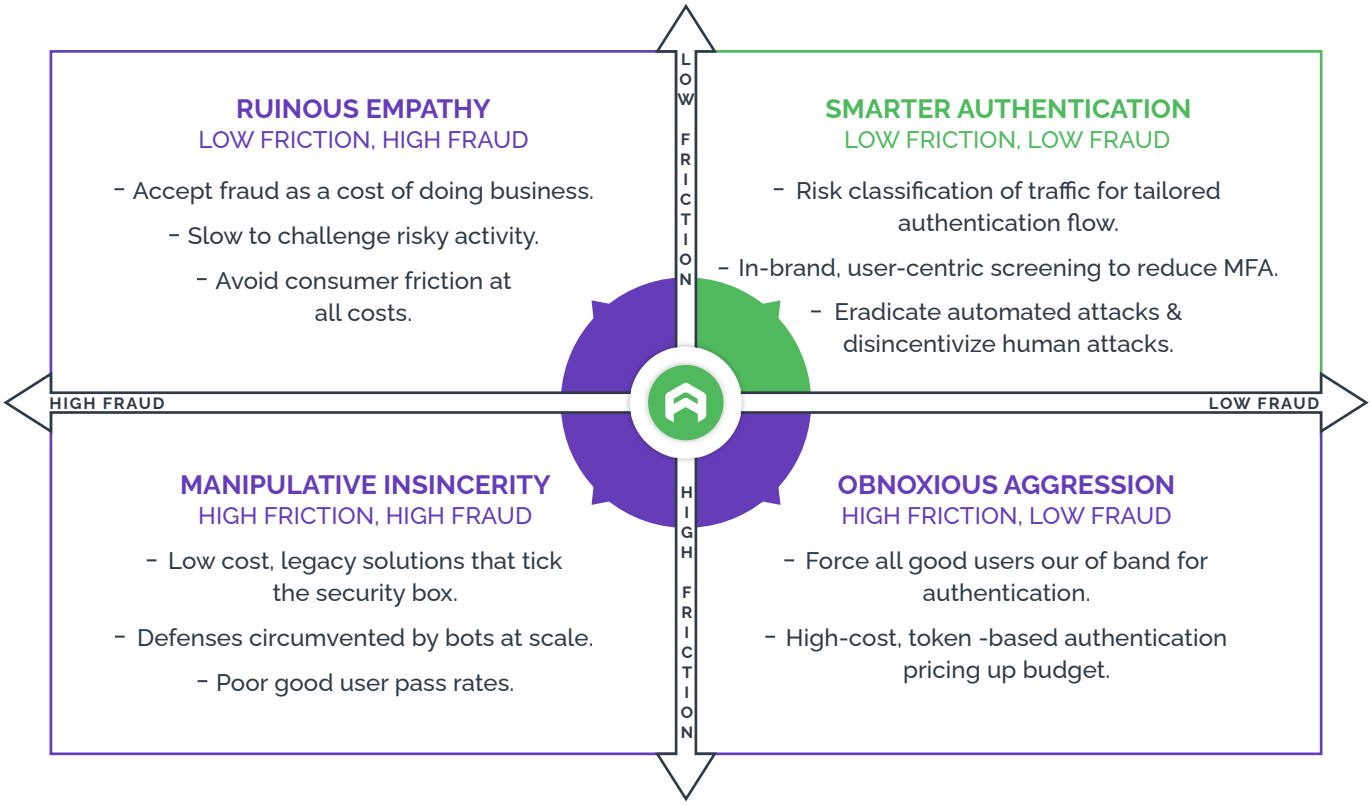
HOW WELL ARE BUSINESSES PREPARED?

Businesses find themselves caught between the competing forces of rising fraud levels and rising customer expectations. Consumers demand security, but show little tolerance for any delays or barriers in their digital transactions.

Some businesses have become too heavy handed, forcing many good users out of band to authenticate, at a great cost to themselves. On the other end of the spectrum, the realization that unnecessary friction kills the commercial goals of a business has led to a backlash against nearly all friction. Being too reluctant to challenge high-risk traffic, and preferring to eat the costs of the potential fraud losses, has set back our collective mission to address fraud.

The correct path forward will always be a blended approach between risk assessments and step-up authentication. However, businesses have been missing a vital intermediary step between flagging risky activity and forcing users out of band to authenticate. Interdiction of higher risk traffic through user-centric challenges that appear within the session can be a vital component in solving the fraud versus friction tug of war.

Targeted friction can deter fraud by rendering attacks unprofitable, without ruining the experience for good user. Friction is a vital component in the user journey safeguarding security, building customer trust, and maintaining company reputation.



ACTION PLAN

- Identify and replace any cheap or legacy security technology that fails to keep UX at the front and center.
- Deploy different levels of screening based on the risk profile, ranging from invisible risk assessments, in-session user challenges, to out of band authentication when absolutely necessary.
- Invest in a continuously learning platform that will learn from past assessments to make smarter decisions about who to challenge in the long run.
- Use machine learning to turbo-charge identification of emerging attack patterns while reducing customer intervention rates, to improve the overall user experience.

CONCLUSION

No one could have anticipated the drastic changes in the digital landscape over the last few years. With businesses operating largely online, this offered a window for opportunistic fraudsters to target weak points in companies' security posture and exploit their services.

But even if 2022 returns us to some semblance of "normal", don't expect fraudsters to just go back to the way things were. These new more frequent and severe attacks are here to stay. By understanding the motivations behind fraud, how the global fraud ecosystem is connected, and how to effectively stop attacks without impacting good users, you can bankrupt the business model of fraud, enable growth and keep customers happy.

Arkose Labs

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers the world's first $1 million credential stuffing warranty. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks while improving good user throughput. Headquartered in San Francisco, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, Tokyo, Japan, and London, UK, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast500 ranking.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

UK • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Schedule Demo