Arkose Labs

UNDERMINING THE ECONOMIC INCENTIVE FOR CYBERCRIME

How to achieve long-term protection by sabotaging attackers' ROI

EBOOK

THE BUSINESS OF CYBERCRIME

The growth of online crime is an ugly and unintended consequence of the digital economy. As more and more consumer interactions become digital, attackers are finding inventive new ways to monetize these customer touchpoints. We have entered an era where online identity cannot be trusted, and intent can easily be faked.

It is said that cybercrime is now more profitable than all of the world's drug trade combined, with annual losses from cybercrime predicted to reach $6 billion by 2021. Losses at this scale could not be achieved by lone attackers working in silos. In fact, the growth of cybercrime has created a parallel ecosystem of businesses, now known as Cybercrime-as-a-Service (CaaS), that supports this activity and shares in the profits.

These CaaS-based activities range from identity farms, which create synthetic identities and test stolen credentials, click farms and sweatshops, which provide humans to carry out nuanced attacks, and 'arms dealers' selling sophisticated tools to launch large-scale complex attacks.

These cybercrime outfits exist because there is relatively easy money to be made with little-to-no risk if done correctly. The attackers' business model is based on their access to the tools, resources and financial incentives to launch and increase attacks, including:


Account Takeovers (ATOs)


New Account Fraud


Fake Reviews


Chargebacks


Spam and Abuse


Inventory Scraping

Implementing security measures to prevent disruptions in these three key areas can lead to significant cost savings and improved ROI for the business. By proactively addressing security vulnerabilities, companies can avoid costly data breaches and reputational damage. Investing in a strong security infrastructure increases efficiency and productivity, resulting in many long-term benefits.

THE SOCIO-ECONOMIC FACTORS DRIVING GLOBAL ATTACKS

Underpinning the attackers' ability to access the required resources to launch successful attacks are global socio-economic factors that impact individuals' appetite to get involved in cybercrime.

Disparities in wages and cost of labor, differing costs of living, and the comparative purchasing power of different currencies shift incentive levels among would-be attackers. For example, based on IMF statistics on purchasing power parity, the Russian ruble is a quarter of the value of the United States dollar. Therefore, cybercriminals in Russia stand to gain four times the value from defrauding U.S. businesses, as opposed to acquiring rubles.

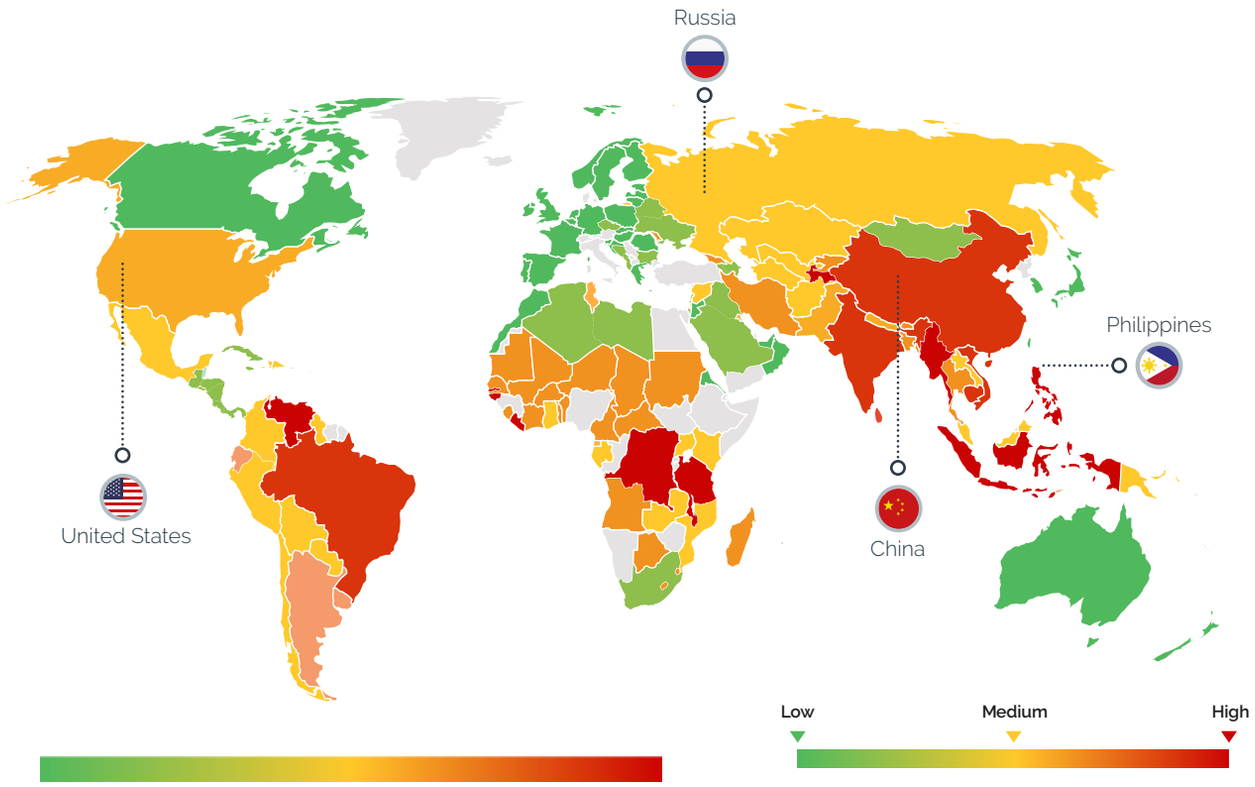
On top of economic drivers, regions have different access to the technology needed to support sustainable cybercrime outfits. For example, while Ethiopia is a country with very weak purchasing power parity, it equally has one of the lowest internet penetration rates globally. With only 15% of the population having access to the internet it is an unlikely cybercrime hub.

Therefore, rather than the very lowest income countries having the greatest incentive to enter the global cybercrime field, it is the lower- and middle-income nations where financial incentive and opportunity converge to make cybercrime most appealing.

Our Attack Incentive Index indicates the areas most susceptible to involvement in cybercrime, both for individuals perpetrating attacks directly and those providing the shadow services which prop up organized fraud operations. This is based on regional economic data alongside intelligence from the Arkose Labs global network, which uses challenge-response data to show the time fraudsters are willing to spend solving step-up challenges before abandoning attacks as they become uneconomical.

We see these dynamics being played out in the real-world attacks detected on the Arkose Labs global network. For example, Russia, the Philippines, and Indonesia all have the highest Attack Incentive Index rating and feature in the top five countries from which attacks originate.

ARKOSE LABS ATTACK INCENTIVE INDEX



United States

We see high levels of domestic attacks on United States businesses, however, fraudsters will abandon attacks early when they need intensive human resources and costs are high.

Russia

Recent surge in attacks from Russia, with a high proportion of human-driven versus automated attacks using low-cost resources.

Philippines

Consistently the top attack originator, fraudsters are driven by the low purchasing power of the region, meaning that there are big gains to be won in defrauding western countries.

China

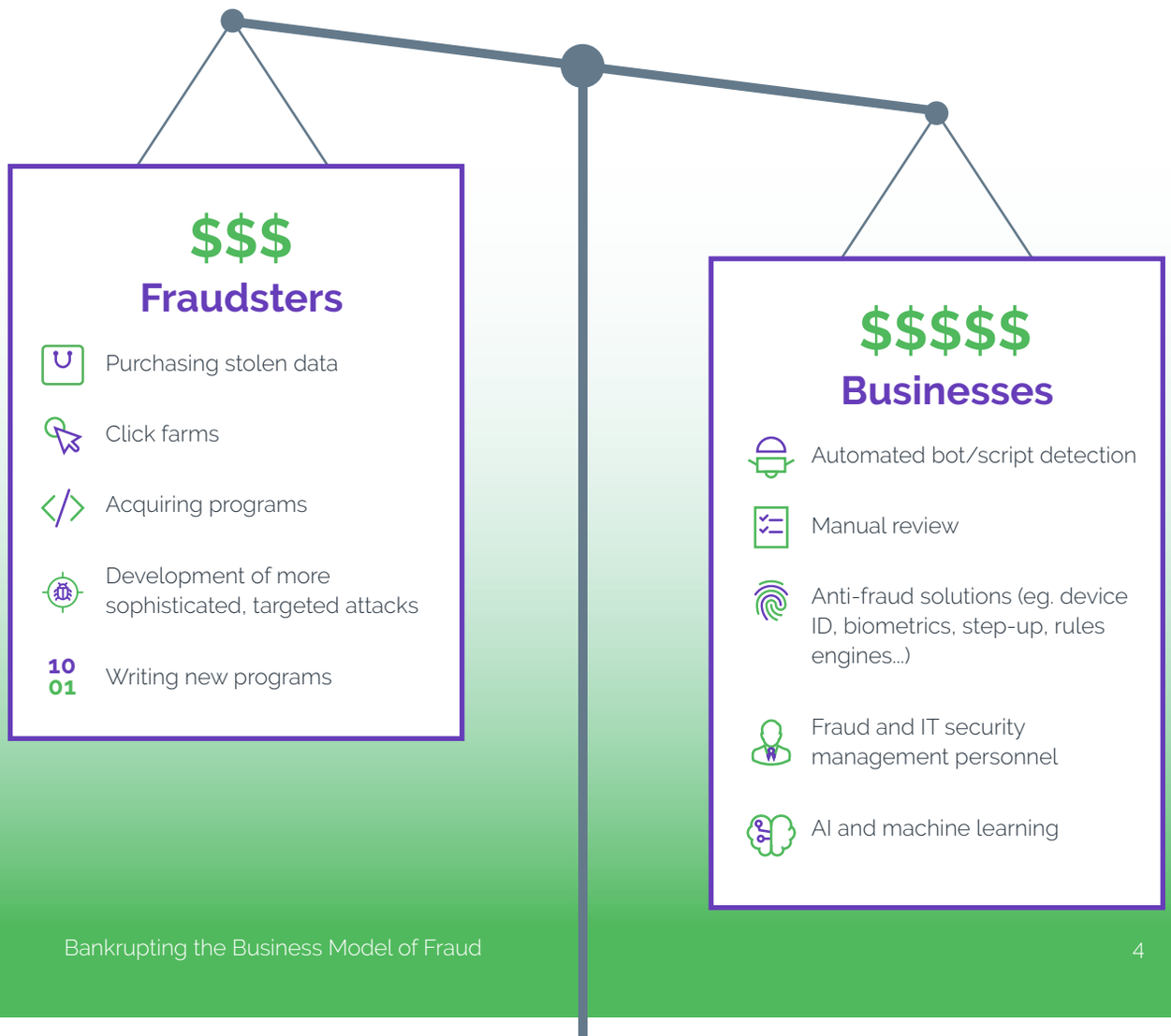
The enormous labor pool available in China leads to a great deal of human-driven fraud and click farms, as fraudsters can still preserve ROI when relying on manpower.

COMPARING THE BALANCE SHEETS

Businesses are coming up against global cybercrime networks which are leveraging regions with high incentive levels, using the economic realities of different locations to their advantage. In recent years, businesses have tried to deploy a range of solutions to protect against these attacks, but sometimes the cost of these tools may outweigh the revenue from those use cases.

While this looks like a surprising amount of outgoing expenses for the fraudsters, they are able to keep costs low by casting their nets globally to tap into markets with very low overheads. While cybercriminals' costs are able to consistently drive profits operating this way, businesses are experiencing ever-expanding demands on their budgets. For a sustained fight against cybercrime to be successful long term, we need to focus on eliminating the economic advantage of fraudsters versus the businesses they target.

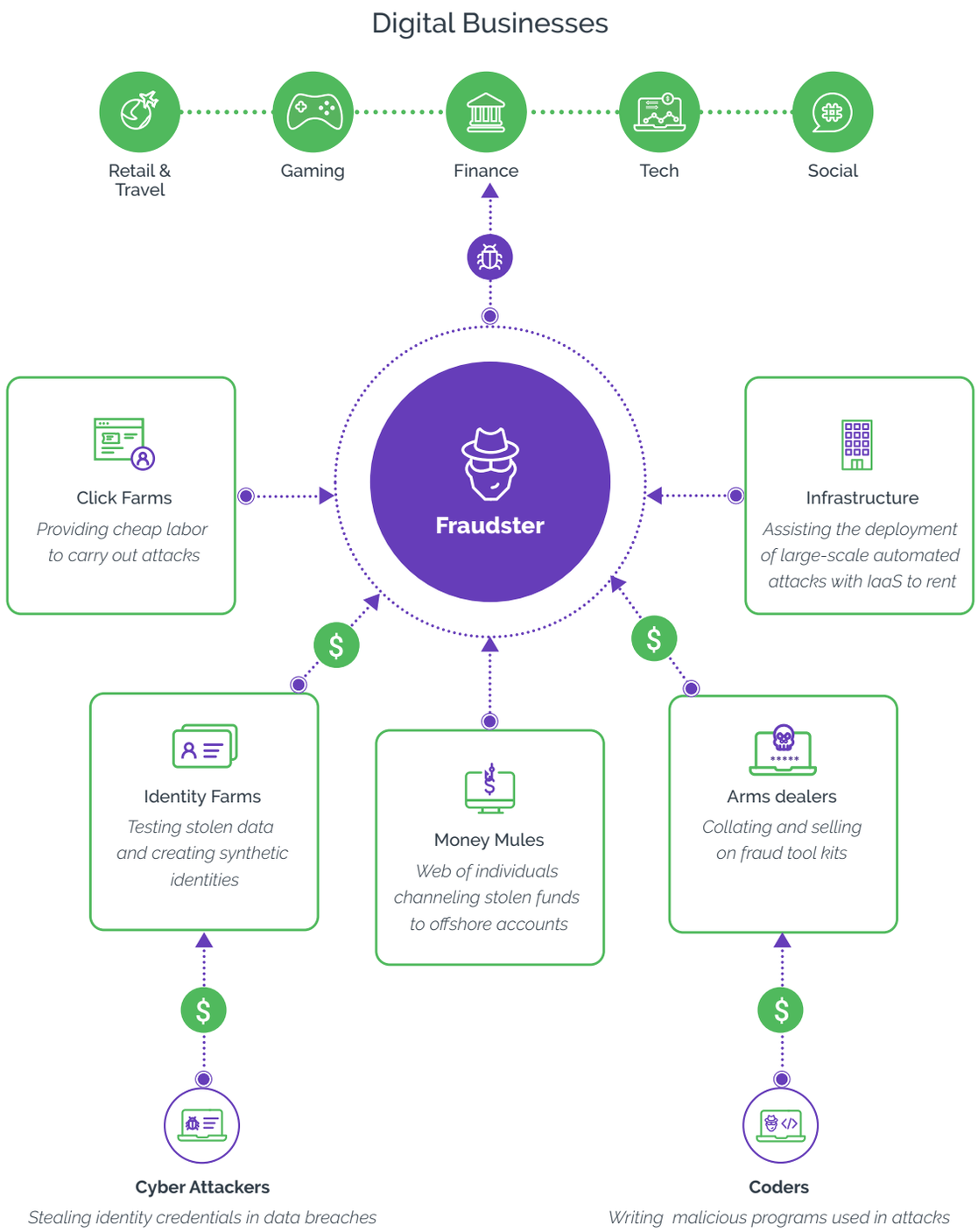
One way businesses are doing this is by investing in advanced technologies that can quickly and effectively detect and prevent attacks. By doing so, organizations can significantly reduce their losses from cybercrime and improve their ROI. Additionally, businesses can leverage economies of scale with offensive and defensive strategies that help mitigate the cost of combating online crime.



FRAUD ECOSYSTEM OF SUPPORT

The ecosystem that has sprung up to support the business of fraud is multi-faceted, with 'services' such as identity farms, click farms and money mules making it possible for large-scale, organized fraud to exist.

These are accessed through the Dark Web, alongside forums which share the latest and greatest tools and techniques that are working against current business defenses.



TOLERANCE OF FRAUD IS UNDERMINING OUR ABILITY TO COMBAT CYBERCRIME

Despite extensive investments in bot detection, device identification and anti-fraud systems, companies have come to consider fraud as an operational cost of doing business. Order acceptance and conversion rates are being prioritized to the point that it has become acceptable to sustain regular fraud losses - as long as these losses are kept below a certain threshold.

The ultimate victims are the end users who then have to spend precious time and resources trying to reclaim their digital presence and undo the damage caused to their finances and credit history.

However, tolerance for fraud across the digital commerce ecosystem is actively incentivising fraudsters given that their operation is built on their ability to aggregate this tolerance across the globe. With each successful attack, fraudsters win and generate funds and financing to continue their operations. This has created a cybercrime cycle of success wherein fraudsters attack, businesses find a way to stop the attack and fraudsters find a way around their defenses. Hence each successful attack further propagates this vicious cycle.

Each successful attack gives the fraudsters a new playbook to replicate across companies, industries and regions until businesses find a way to stop it. This global knowledge sharing between fraudsters means that fraud and risk management departments are on the back foot, as any gaps and vulnerabilities in their platform are quickly identified and globally exploited by the fraudsters.

THE CYBERCRIME CYCLE OF SUCCESS

The more successful attacks that take place, the better the fraud community's ability to launch future attacks. As a result, fraud attack rates are steadily rising – despite the numerous anti-fraud measures deployed in many digital businesses.

Preliminary attacks

Test stolen data & newly purchased toolkits

Larger-scale attacks

Target more business with verified data and toolkits

New data & more sophisticated toolkits

Proceeds used to buy fresh credentials and new toolkits to evade anti-fraud measures

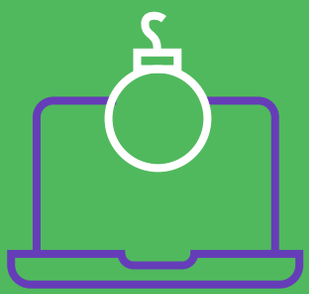
Increased attacks from multiple perpetrators

Knowledge-sharing among fraudsters on tools & techniques which are effective spurs on increased attacks

HOW DO WE BANKRUPT THE BUSINESS MODEL OF FRAUD?

Fraud levels will continue to rise indefinitely unless businesses stop tolerating fraud as a 'cost of doing business'. Allowing for a certain level of fraud within your online operations actively feeds future attacks, by allowing fraudsters to continually improve their ability to launch and expand successful attacks.

Instead, we must focus on disrupting fraud to the point that it ceases to be a lucrative option for cybercriminals, no matter where they are in the globe. This requires targeted action that increases the costs involved for fraudsters to launch attacks, increases the strain on the resources required to carry out attacks, and shifting the attack surface.



STEP 1

DISRUPT CYBERCRIMINALS' TOOLS

As things stand, fraudsters are able to share data and scripted attacks freely among themselves to attack multiple businesses. These tools are often tested on one company's website and, if they prove successful, rolled out at scale across the digital commerce landscape.

Taking down these tools requires businesses to move beyond an arms-race mentality, to focus on the steps which will increase the time, cost and effort it takes for fraudsters to carry out attacks. By increasing the burden in these three areas, it will lead to more bad actors abandoning the process earlier.

Businesses must deploy sophisticated analysis of traffic from the very beginning of the customer journey in order to triage between legitimate customer behaviour and suspicious activity. Whereas trusted customers are provided with a seamless, friction-free journey, those sessions which raise red flags can then be sent to targeted step-up authentication.

Sharing intelligence among trusted businesses can ensure that existing attacks cannot be copy-and-pasted across different organizations. This drives up the time and investment needed from fraudsters to launch successful attacks, in turn hitting their return on investment (ROI).

When fraudsters are required to dig deeper into their pockets to access effective tools, it renders fraud all the less appealing.

STEP 2

INCREASE THE STRAIN ON FRAUDSTERS' RESOURCES

A lot of fraud focuses on high-velocity, low-value gains across enough businesses to drive a significant profit. Automation is key to being able to carry this out at the scale and cost-effectively. Even with access to low-cost resources from areas of the globe with high Attack Incentive Index rates, it is still an impractical option to require human interaction every time you deploy a fraudulent attack.

Focusing on defenses that ensure fraudsters require a real human being behind every single attack is a surefire way to undermine the financial incentive to perpetrate fraud, by putting increased strain on their resources and slashing potential ROI.

Adaptive step-up challenges which are targeted at suspicious traffic, wipe out attacks that rely on automated-only tactics. Effective solutions are those which keep moving the type of challenge presented in order to keep moving the goalposts and prevent fraudsters scripting their way round your defenses to carry out duplicate attacks.

When they need more fingers on keypads and eyes on screens to bypass puzzles and challenges that only a human can decipher, this dramatically drives up the manpower and the costs required to carry out attacks. The bottom line is that when you sap the fraudsters resources, make a dent in their ROI and undermine the financial incentive behind fraud, they will turn to other methods of making cash.

STEP 3

SHIFT THE ATTACK SURFACE

Fraudsters rely on being able to control decision points when on a business' digital property and deploying the appropriate tactics to evade established anti-fraud measures. They are skilled at masquerading as legitimate consumers using hijacked devices, stolen identities and obfuscating their IP address and other identifiers in single request attacks.

In order to take the control away from fraudsters, we need to shift the attack surface by redirecting suspicious sessions to an intermediate platform which provides independent verification of identity. This provides a buffer between the fraudsters and the sites they are so practiced in attacking, rewriting the rulebook on how to successfully launch attacks.

Reclaiming control of these decision points means fraudsters will quickly become frustrated when their tried and tested methods cease to work. When they can no longer fall back on their existing arsenal of automated tools, stolen identities and click farms will lead to escalating costs for reduced gains, removing the financial motivation behind organized fraud.

HOW DOES ARKOSE LABS HELP BANKRUPT THE BUSINESS OF FRAUD?

Arkose Labs believes that combating the growing online fraud epidemic requires a solution rooted in prevention and stopping abusive attacks at the point of entry without disrupting user experience. Our approach helps stop the vicious cycle and puts the control back into the hands of the digital businesses:

1. Shifting the attack surface:

Arkose Labs' approach shifts the attack surface from the business to our platform so that fraudsters are no longer attacking a particular use case/customer touch point but are being subject to smart and intelligent friction that saps their resources. Because of this, the businesses don't need to divert their precious resources to deal with the attacks, while benefiting from the shared attack pattern intelligence that Arkose Labs brings (from the insights from past attacks on the Arkose Labs platform).

2. Breaking down the fraudsters' business economics:

Arkose Labs' approach makes attacks more difficult and costly, which disrupts the fraudsters' economic incentive and breaks their business model. This results in a longer term solution and stops the cat-and-mouse game that fraudsters play with businesses.

3. Longer term impact:

Since fraudsters are in this to make money, they try to quickly pivot each time their attacks are thwarted. With Arkose Labs, they not only are unable to bypass the platform but end up spending a lot of resources trying unsuccessfully to do that. This results in a success for the entire digital commerce ecosystem as there is one less operator trying to dupe businesses and customers.

4. Data network effect:

This approach not only delivers a sustainable solution to businesses against fraudsters but also helps the fraud and risk management ecosystem benefit as each attack provides insights into the fraudsters' operations, augmenting the overall network intelligence.

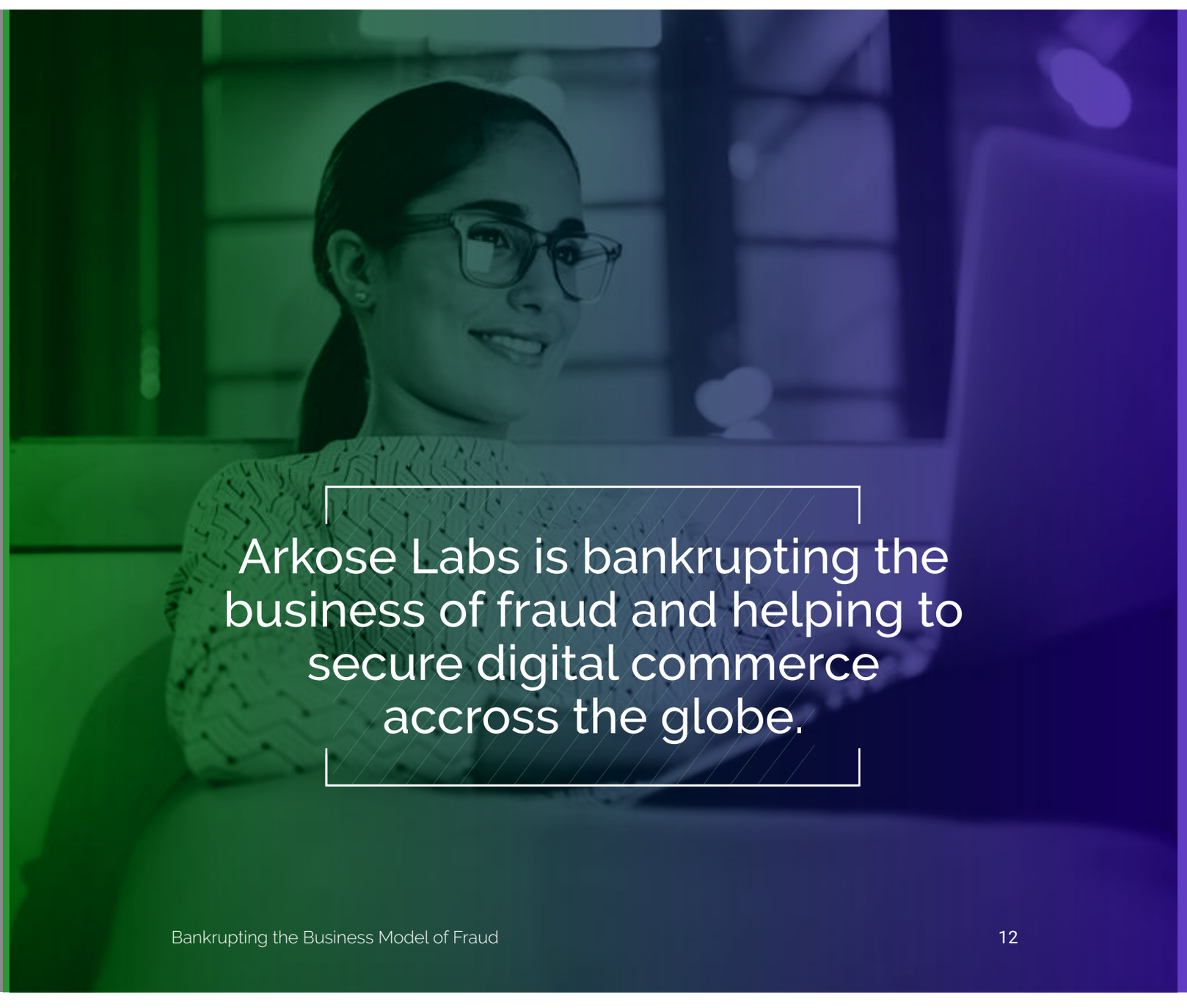
5. Continuous learning:

Our decision engine and enforcement challenges learn from newer attack patterns. This shifts the power from the fraudsters to the businesses, and benefits the overall digital commerce ecosystem.

CONCLUSION

Perpetrators of fraud who are purely motivated by financial gain can only sustain their operations when the cost of executing abuse is less than the revenue that can be extracted. By focusing on prevention controls which render fraud more costly and time-consuming, it will cease to become an attractive prospect as the risks heighten and rewards decrease.

While many businesses have come to accept fraud as an operational cost of doing business in the digital age, we believe that the only long-term approach to curbing cybercrime is to adopt a zero-tolerance approach which focuses on disrupting the economic drivers leading individuals to cybercrime. Companies on the Arkose Labs platform benefit from this zero-tolerance approach, with a 100% Service Level Agreement (SLA) guaranteeing protection against large-scale attacks.



Arkose Labs

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M credential stuffing and SMS toll fraud warranties. Its AI-powered platform combines powerful risk assessments with dynamic attack response to undermine the strategy of attack, all the while improving good user throughput. Headquartered in San Mateo, CA with offices in London, Costa Rica, and Brisbane, Australia, Arkose Labs protects enterprises from cybercrime and abuse.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 2 W 5th Ave, Fl 3, San Mateo, CA. 94402
Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006
UK • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF
Costa Rica • San José, Escazú, San Rafael, Escazú, Village Torre II

Schedule Demo