Arkose Labs

Busting the ROI of Fintech Fraud

Navigating a complex threat landscape for banking and lending fintechs

The New Face Of Financial Services

An industry like no other, fintech is an engine of innovation that is rewriting the rule book on how consumers around the globe access financial services.

A wide array of dynamic providers have emerged, with digital and mobile-only banks and online lenders making the biggest splash. Lines are blurring between traditional banking and fintech, with more and more brick-and-mortar banks embracing digital services and integrating with fintechs through open banking.

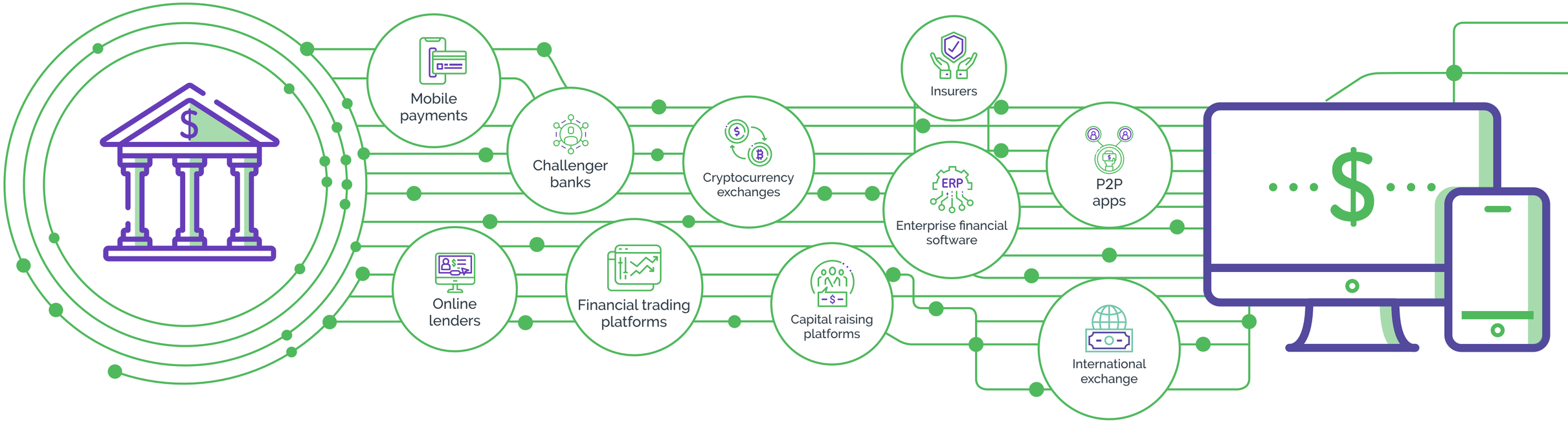
A major impact of the fintech revolution has been the speed at which banking and lending decisions are made, with consumers expecting instant access to new financial products. This presents unique challenges when protecting their digital properties against organized fraud.

Fintechs face a complex and highly organized cybercrime ecosystem. The 2019 Official Annual Cybercrime Report predicted that by 2021 cybercrime will cause annual losses of $6 trillion globally. The high ROI potential for fraudsters targeting the finance sector means that internal fraud prevention teams are under major strain as they keep up with the ever-evolving nature of fraud.

Fintechs must fight fraud on multiple fronts while delivering a streamlined user-friendly product. These digital-born companies have the opportunity to take a fresh approach to effective fraud prevention, enabling them to stay nimble and scale rapidly, while preserving the all-important trust factor.

An Explosion In Banking And Lending Start-Ups

The evolving fintech landscape provides innovative and user-focused alternatives to legacy banking options. They are both in competition and 'coopetition' with traditional financial institutions. Their value has been recognised by the private equity markets, and fintechs have received 25% of all investments by venture capitalists and start-up funding in 2019. Fintech IPOs had a total valuation of $22.5 billion by June 2019.*



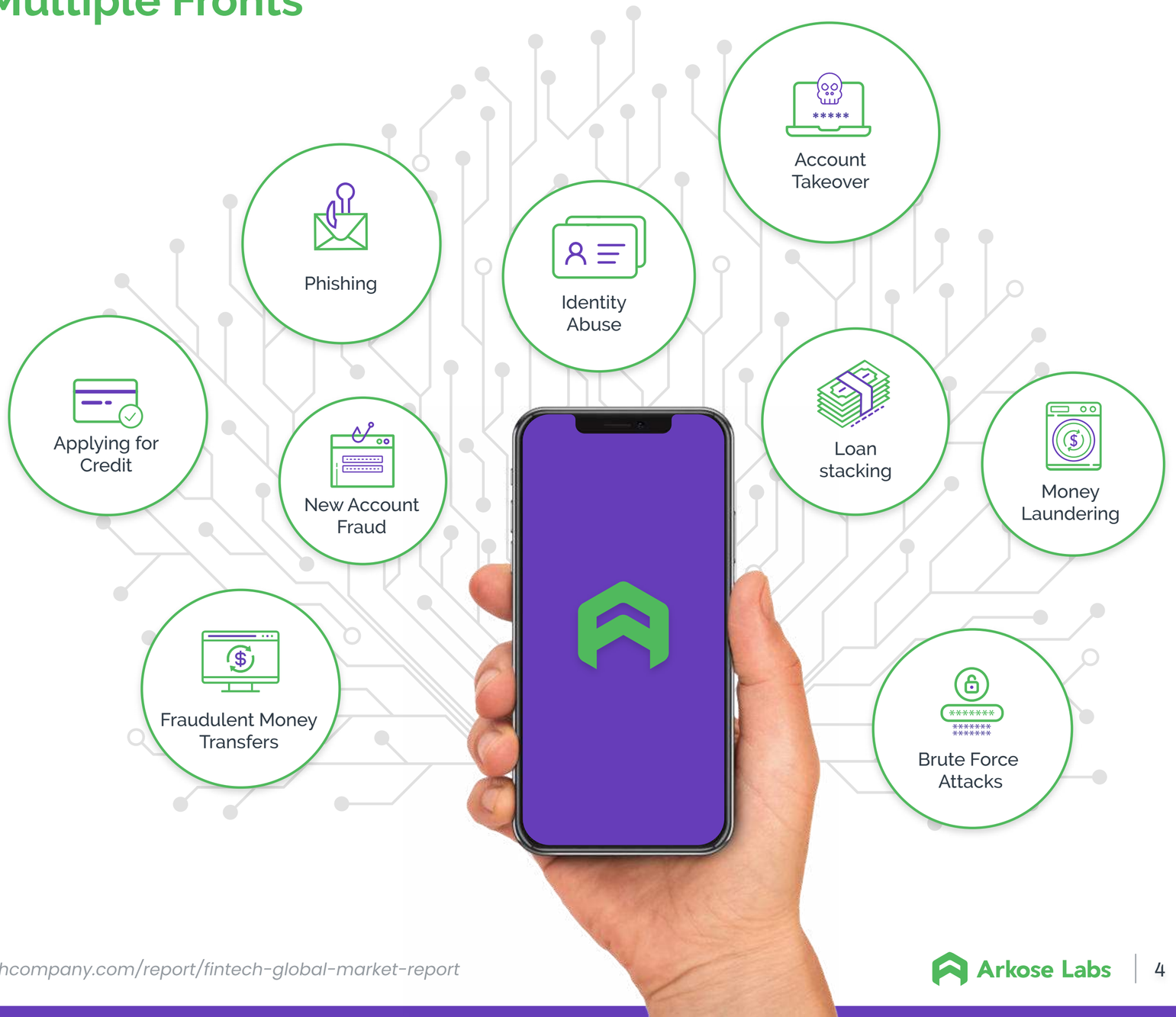
*(http://www.imf.org/external/pp/ppindex.aspx).

Fintechs Face Attacks On Multiple Fronts

The global fintech market is predicted to grow to $310 billion at an annual growth rate of 24.8% through 2022*. This offers a wealth of positive aspects for customers worldwide, but also increases the attack surface for fraudsters targeting financial transactions.

A shadow cybercrime ecosystem has expanded to attack these businesses from every angle. Fraudsters have developed sophisticated attack patterns that confound traditional fraud prevention solutions. They learn from previous failed attacks, and invest considerable resources in staying ahead of fraud prevention strategies.

Fraudsters use a multitude of tools to obscure their attacks, and to blend fraudulent activity in with legitimate user behavior.



*Fintech Global Market Report - https://www.thebusinessresearchcompany.com/report/fintech-global-market-report

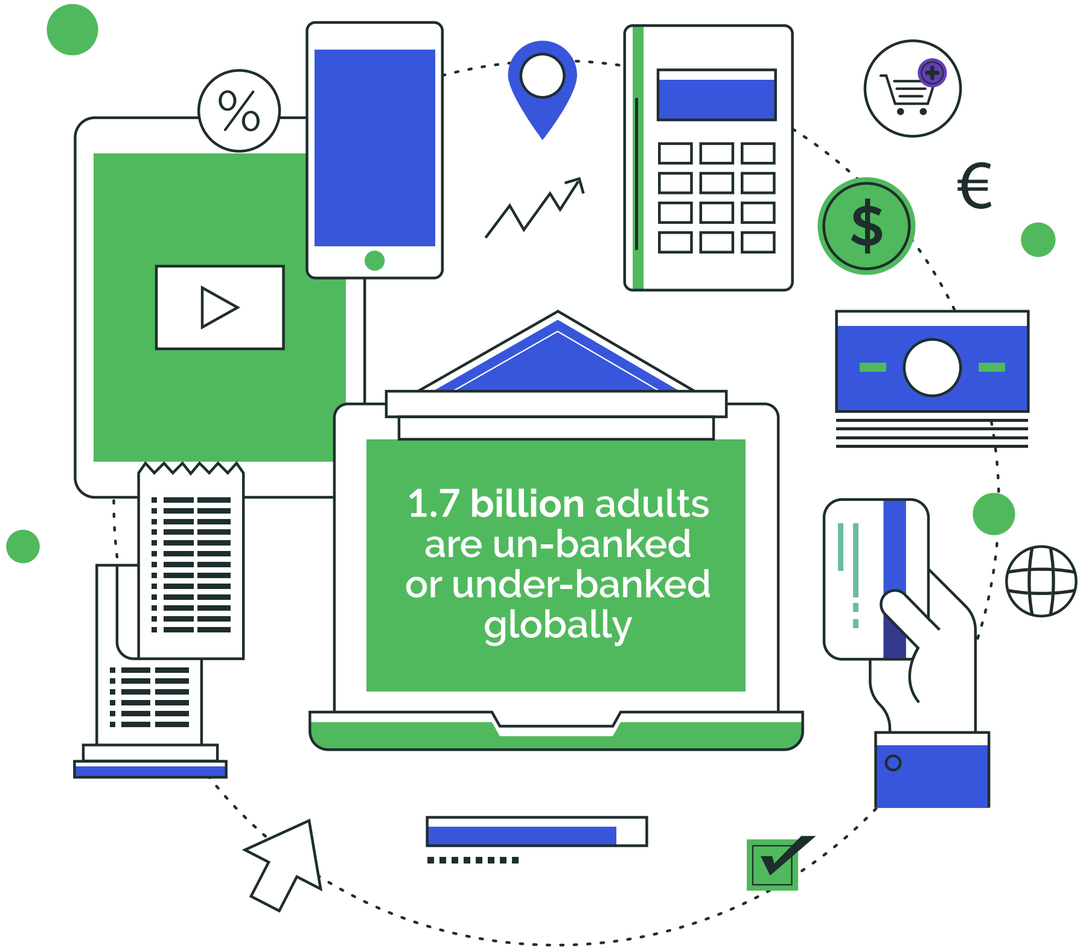
Fintechs Are Driving Global Financial Inclusion

Fintechs can offer financial services to individuals typically excluded from traditional banking

The issue of un-banked and under-banked individuals is a major obstacle to social mobility and financial stability. Fintechs are uniquely positioned to be able to expand access to financial services to these individuals. WIth lower overheads than traditional banking, they can tap into this global market by offering low-cost products to individuals, including micro-loans, investment and financial risk management.

Where thin-file individuals have little or no credit history, fintechs can access data from vendors' real-time transactions on commercial platforms allowing them to assess risk on a micro-basis. Through e-payments and money transfer services, fintechs can offer quick, low-cost transfers that provide large savings for those with the biggest need. This has a huge impact on individuals working abroad and sending money home to less-economically stable countries.

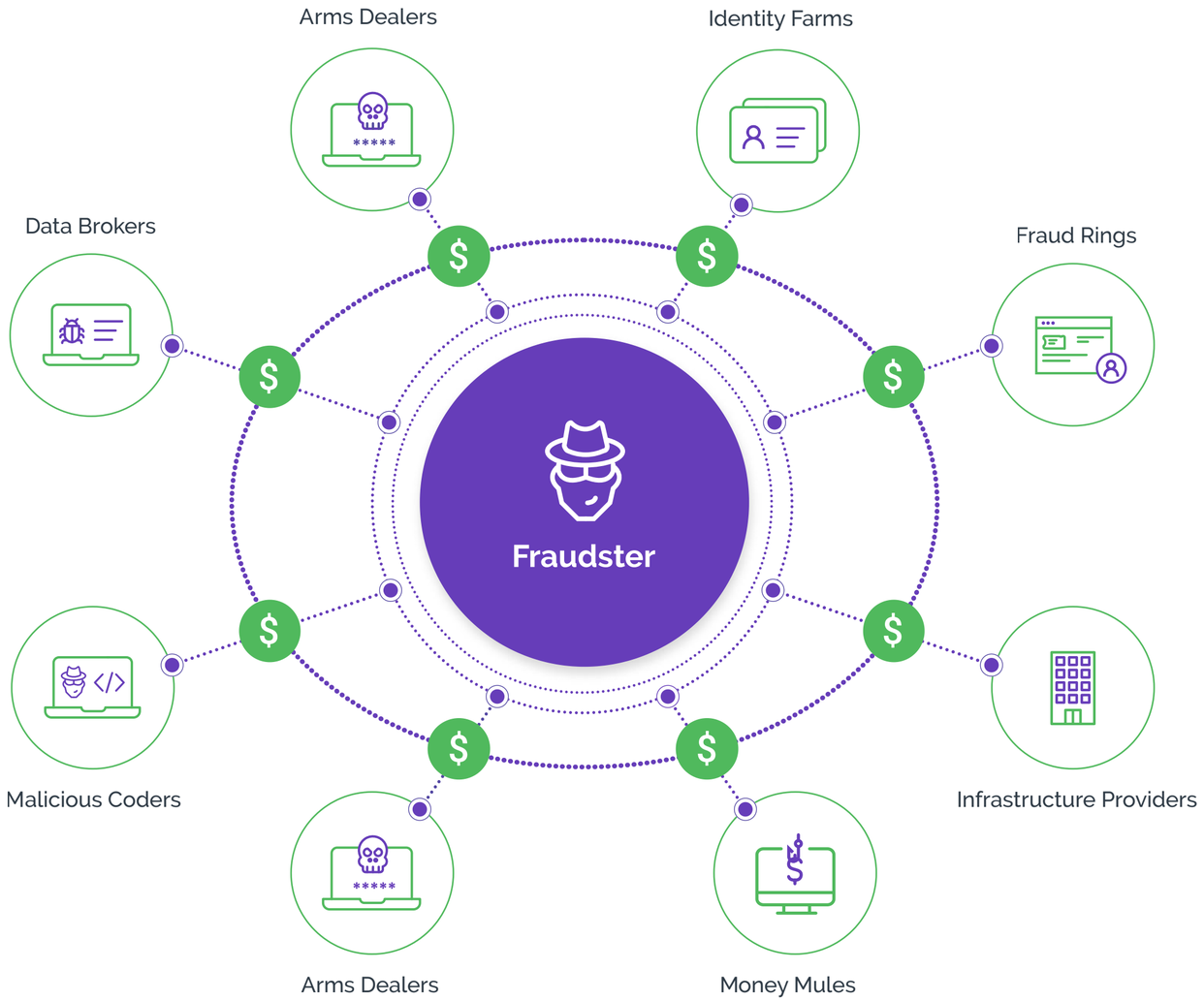
Global digital intelligence is playing a vital role in opening financial services up to the least privileged, and encouraging growth in developing economies.



Start-Ups Versus A Mature Global Cybercrime Ecosystem

Fast-growth fintechs are facing a well developed, inter-connected fraud ecosystem, which has honed its tactics and techniques after years of targeting traditional financial institutions.

Fraudsters can tap into a range of services and data for sale: identity farms, which provide verified, complete identity profiles; vendors of sophisticated fraud toolkits; and sweatshops offering human resources to carry out attacks from low-cost regions such as South East Asia. Additionally, fraudsters have developed highly effective bots that mimic human activity and easily bypass traditional fraud solutions.



Building And Preserving Trust In Fintech

As challenger banks and online lenders strive to establish credibility, competing with established institutions who have dominated the market for decades, establishing and maintaining customer trust is 100% central to their commercial success. As consumers sign up to new services and make transactions on these emerging platforms, every interaction they have goes to either build or erode.

ADDING TO TRUST

- Seamless user experience
- Robust fraud protection
- Low-friction authentication for genuine customers
- Easy access to customer support teams
- Transparent guidelines on fraud prevention

THREATS TO TRUST

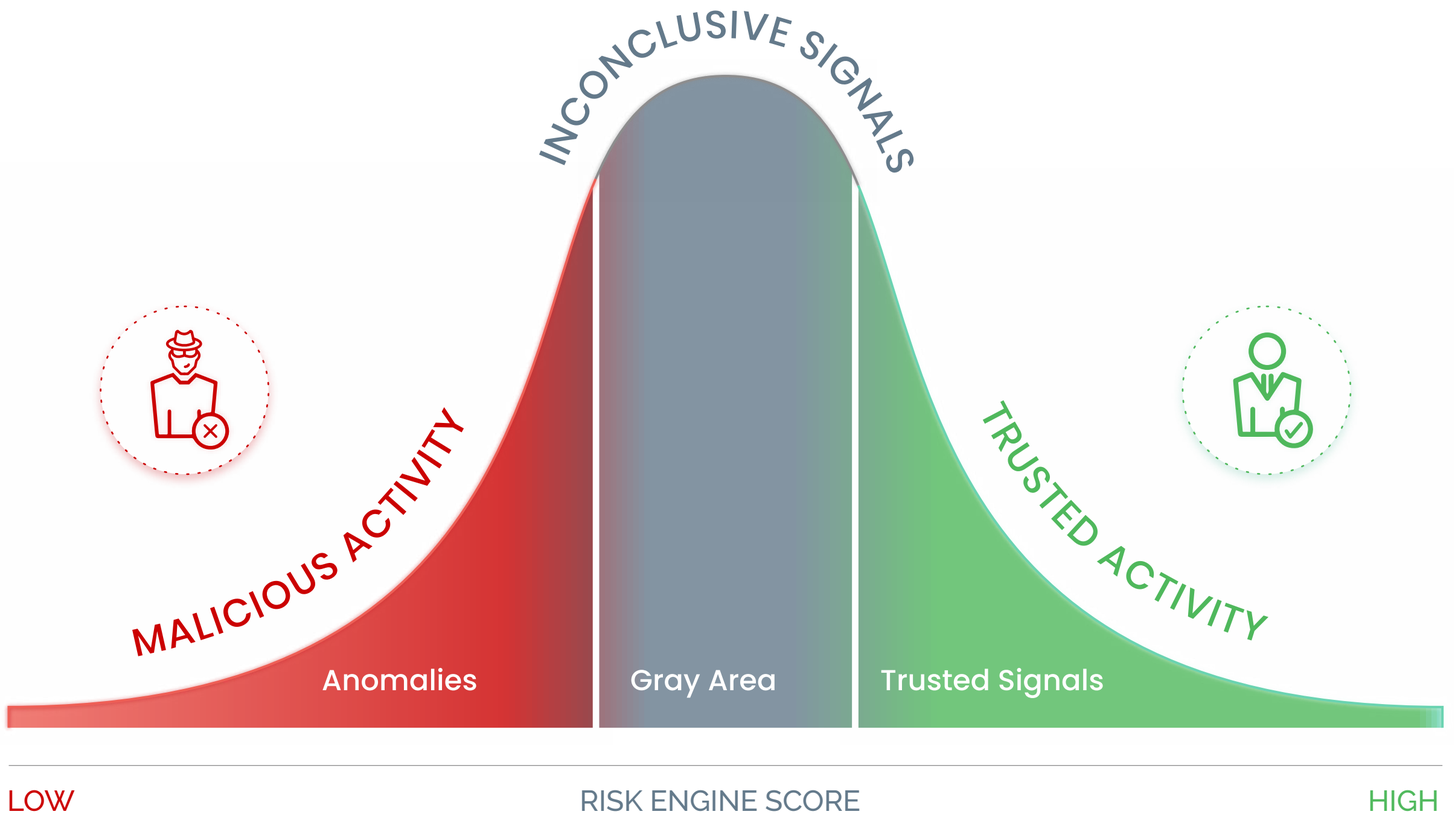
- Experiencing fraud on websites and apps
- Out of band authorization that makes users jump through hoops to prove who they are
- Being a victim to account takeover
- Encountering limited or difficult access to support
- Failing verification challenges and being blocked in error

Navigating Unpredictable Fraud Signals In A Complex Threat Landscape

The corruption of digital identities makes it difficult to accurately differentiate between consumers and fraudsters purely through data-driven analysis. There is a growing 'gray area' between traffic that is recognized as trusted and that which is fraudulent.

Fraudsters have data at their disposal and highly developed tools that can deceive traditional fraud solutions. Genuine consumers can also display unpredictable behavior.

Fintechs are set up to process high numbers of applications quickly, and approve transactions in an automated, hands-off way. The growing gray area means that it is increasingly difficult to achieve this without leaving the business vulnerable to fraud or placing a heavy burden on in-house teams.



Digital Identities Have Been Corrupted At Scale

As exclusively online and mobile businesses, fintechs are more reliant than other sectors on verifying the identity of users, without onerous identity proofing processes.

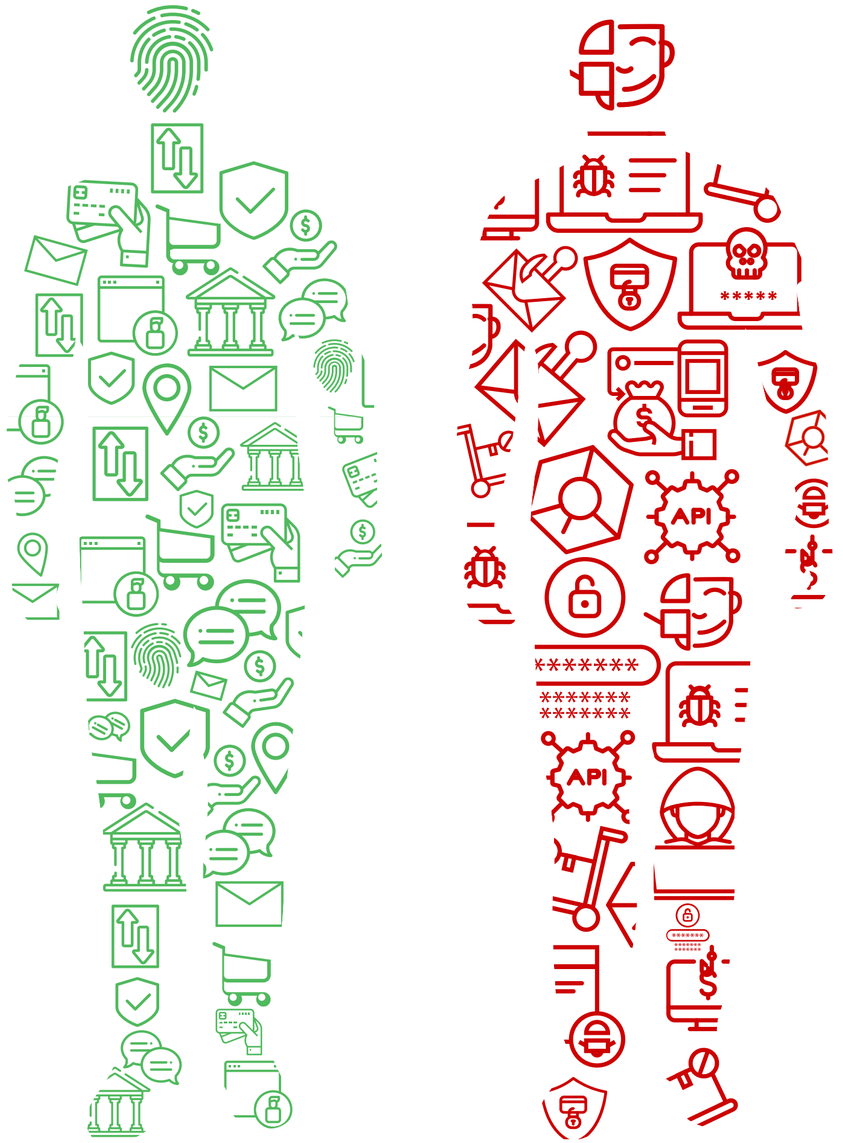
However, digital identity information has largely been compromised. Armed with accurate knowledge of the fraud detection parameters used to identify online abuse, fraudsters are able to use their own defenses against the businesses they attack in order to masquerade convincingly as trusted consumers.

Breached identity credentials: Fraudsters use wholesale 'identity farms' to access large pools of stolen and synthesized identity credentials.

Device intelligence: Fraudsters purchase cloned fingerprints of trusted devices to mimic good users, or use randomization tools to make stolen devices seem new.

IP address & location: Fraudsters use increasingly sophisticated location spoofing tools that enable them to appear as if they are a trusted source.

Behavior analytics: Fraudsters gain insight into the behavior patterns of genuine customers from previous account takeover and use attempts, and use this to circumvent anti-fraud measures.



The Rise Of Sweatshop-Driven New Account Fraud

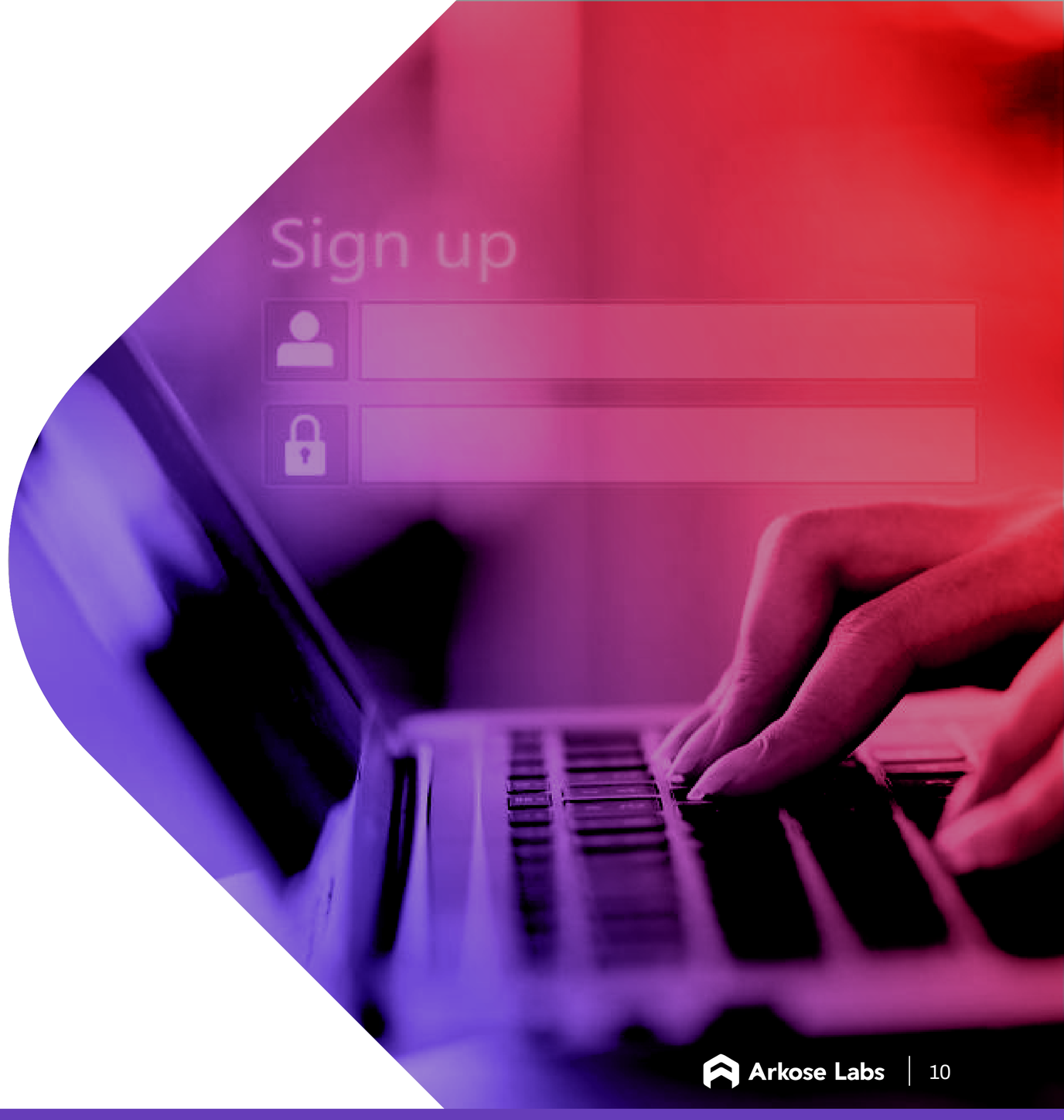
New account fraud is the most attacked customer touchpoint on Arkose Labs' network.

Fast-growth fintechs spend a lot of marketing dollars creating a buzz around their business, with pressure to meet high customer acquisition targets.

They invest heavily in business expansion offering:

- Attractive promotional deals for new account holders.
- Easy access to credit and other financial services.
- Simple account application procedures.
- Account access through a mobile phone app.

Fraudsters actively exploit this, with automated attacks augmented with human sweatshops which impersonate genuine users, to create new accounts at scale.



The High Stakes Game Of Account Takeover

Accessing financial accounts through account takeover allows fraudsters to commit serious cybercrimes, affecting both individual users and wider society.

- Money laundering and money muling
- Password and payment details theft
- Account draining
- Fund organized crime
- Fraudulent credit applications

Fraudsters are using stolen data and corrupted digital identities to mount attacks at scale. Highly sophisticated bots easily bypass traditional fraud prevention solutions using data harvested from previous failed attempts to evolve and improve.

Additionally, as fraud prevention technology evolves, criminals are increasingly employing cheap human labor in developing economies to turbo-charge attacks. Arkose Labs found that human-driven attacks increased by 33 percent at the end of 2019.

Businesses need a multi-layered approach that differentiates between human and bot-driven account fraud.

Cashing Out: Payment Fraud For Fintechs

Fintechs are especially vulnerable to payment fraud, as fraudsters exploit the new products they have brought to the market.

Fraudsters target multiple payment channels:

- CNP transactions using stolen card details
- Gift card abuse
- Unauthorized money transfers
- Abuse of stored payment details accessed through account takeovers

Companies face the challenge of preventing payment fraud whilst ensuring positive customer experience. The flexibility and accessibility not makes fintechs so attractive not has left them exposed to cybercrime.

To continue making inroads into markets dominated by traditional banking, fintechs need to ensure that they remain innovative and maintain customer trust. Service users need to be able to carry out actions such as instant payments with confidence. Companies need robust authentication methods that don't damage the experience for genuine customers.

Four Key Steps To Tackle Fintech Fraud

Money is the Root of All Fraud

The digital and mobile revolution has allowed fintechs to flourish, with the global fintech market growing at about 25% year-on-year.[1]

However, the risk to fintechs from cybercrime has grown in parallel with their success. Many businesses have focused on mitigation strategies in the face of evolving cyber fraud, while allowing a certain level of fraud to exist - seen as a "cost of doing business in a digital world". This has given fraudsters the financial incentive to continue and grow their operations.

Businesses have been investing in cybersecurity, yet despite expanding budgets and growing fraud personnel fraud rates continue to rise. Rather than throwing more money and technology at the problem indefinitely, businesses need to reassess their strategy.

Many fintechs are in a precarious position whereby they cannot tolerate any fraud on their platforms, due to the negative consequences of any breakdown in trust. Fintechs need a zero-tolerance approach to fraud which defeats the long-term drivers.

[1] *www.statista.com/statistics/617136/digital-population-worldwide/*
[2] *www.prnewswire.com/news-releases/global-fintech-market-value-is-expected-to-reach-309-98-billion-at-a-cagr-of-24-8-through-2022--300926069.html*
[3] *www.cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*
[4] *www3.weforum.org/docs/wef_global_risks_report_2019.pdf*

Step 1

Build Trust With Intelligent Friction

Combine targeted step-up with digital intelligence in the fight against fraudsters.

Many fintechs looking to ensure maximum protection against fraud, alongside minimal intervention rates, are reassessing the role of friction as a positive component in the user journey. When reserved for riskier traffic and using methods which are easy for legitimate individuals to complete, it can help preserve trust and demonstrate that robust steps are being taken to protect against online abuse.

Businesses require a multi-step system that provides:

- Detailed risk assessment of each user based on deep device analytics
- Step-up challenges which are tailored to users risk profile
- Authentication that allows genuine customers to pass unchallenged or easily clear challenges to preserve user throughput

Step 2

Shift The Attack Surface

Disrupt fraudsters' attack methods and relieve the burden on in-house teams.

Fintech need to shift the attack surface away from their frontline businesses and onto a third party platform. Independent verification of identity avoids draining in-house fraud prevention resources and provides a buffer between the fraudsters and the sites they are so practiced in attacking.

Benefits of shifting the attack surface:

- Fraudsters no longer attack their targeted customer touchpoint but are diverted to intelligent step-up challenges
- The projected attack route is disrupted, hampering fraudsters' ability to execute as planned
- Businesses avoid the need to divert their internal resources to deal with

Step 3

Keep Moving The Goal Posts

Stay ahead of cybercrime with future-proof protection.

Fraudsters have learnt to circumnavigate data-driven fraud prevention systems, and use automation to bypass many step-up authentication challenges at scale.

The most effective defenses are those which are by-design constantly evolving in order to keep moving the goal posts for fraudsters. For example, Arkose Labs' approach to image-based authentication is to use proprietary visuals that are continuously changing and tested to ensure they are resilient to being circumvented by the latest machine learning methods.

The traits of successful authentication systems include:

- A constant feedback loop between risk-based profiling and enforcement challenges to keep ahead of emerging threats
- Challenges derived from proprietary visual data to prevent them from being solved using automated tools
- Graduated challenges that are constantly evolving in type and severity and adapt to the risk profile of traffic

Step 4

Streamline The Fraud Prevention Technology Stack

Safeguard the key advantage of nimble fintechs by keeping fraud operational costs and complexity to a minimum.

Traditional banks have complex technology stacks, protecting legacy applications and systems that have built up over time. Managing the alerts and data streams without disrupting their critical infrastructure is challenging and resource-intensive.

Fintechs have a distinct advantage: they are able to implement streamlined fraud operations which use the latest best practice. By leveraging external data sources and validation technologies with their own insights built up on their customer base, robust fraud protection can be put in place.

To keep ahead of the curve, fintech need to balance technology that is easy to implement with a heavy reliance on SaaS products which incorporate:

- Real-time intelligence
- Step-up authentication
- Risk-based decisioning
- Simplified integration and deployment

A Digital-Born Fraud Solution For Fintechs

Fintechs looking to differentiate their offerings face the major challenge of delivering instant decisioning for consumers accessing or applying for financial products, without ever compromising security.

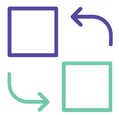
Arkose Labs' platform is tailor-made for companies looking to deliver a stand-out user experience, while retaining a zero-tolerance approach towards fraud and abuse. It is the only platform to seamlessly combine risk-based and step-up authentication, with a continuous feedback loop which makes it the fastest-learning fraud defense platform on the market.

In a world where digital identities have been corrupted and fraudsters have access to highly sophisticated tools, Arkose Labs is combatting the growing online fraud epidemic by undermining the economic incentive behind fraud. Its patented platform accurately identifies bad actors and presents incremental step-up challenges which wear them down and diminish their ROI, without negatively impacting legitimate consumers.

Risky traffic is presented with unique step-up challenges which provide a fun and easy way for customers to prove who they are. For fraudsters on the other hand, these challenges eliminate all automated attacks and prevent human-driven attacks from scaling.

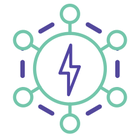
The Arkose Advantage

Arkose Labs has been designed to combat fraud in the post-breach era. By significantly increasing the labor involved in clearing challenges it breaks the business model behind organized fraud. Arkose Labs' two-step platform, Arkose Detect and Arkose Enforce work in tandem, each part of a continuous feedback loop to ensure real-time protection. This provides fintechs with long-term sustainable fraud protection.



Intermediary Platform Buffers Attacks
Independent verification of the authenticity of traffic to shift the attack surface.

Protects Against Automated Attacks
The Arkose Labs 'Acid Test' challenge causes all automated attacks to spontaneously fail.



Lightening-Fast Deployment
Cuts through the complexity with a solution that is easy to install and simple to manage.

Drains Fraudsters' Time and Resources
Renders attacks more difficult and costly to fraudsters, which disrupts their economic incentives.

Continuous Intelligence
Helps the fraud and risk management ecosystem by learning from new attack patterns and providing insights into fraud operations.

Zero-Tolerance Approach
Prevents fraudsters from bypassing its platform at scale using automation or sweatshops.

Busting The ROI Of Fintech Fraud

Fintech has opened up many avenues in the world of finance and as a result has become a lucrative target for fraudsters, who will always chase the money. Spurred on by the rapid expansion of the sector, fraudsters are developing increasingly sophisticated attack patterns.

Fast-growth organizations are struggling to keep on top of the fight against fraud in a way that is sustainable and avoids a never-ending cat and mouse game with fraudsters. In order to disrupt fraud in the long-term, fintechs need to address the economic drivers behind attacks. If a fraudster meets enough resistance, though controls which cannot be circumvented at scale through automation, they will abandon attacks before their ROI is completely eroded.

Businesses need to combine sophisticated risk decisioning, which digs deeps for even the most subtle signs of fraud, with intelligent step-up authentication that adapts to the risk profile of traffic. To avoid getting bogged down by complexity, fraud prevention solutions need to be integrated into existing frameworks and build trust with genuine users - without introducing unnecessary friction.

Only by deploying authentication steps which are are constantly evolving will fintechs stay ahead of emerging attack patterns and stamp out large-scale attacks from bots and malicious humans.

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