Arkose Labs

Top 5 Fraud and Security Steps for Buy Now Pay Later Platforms

Navigating a complex digital threat landscape for lenders

The New Face Of Digital Lending

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 big part of that innovation is the advent of buy now pay later services. Buy now pay later services, commonly known as BNPL, have seen a stratospheric rise in popularity over the last few years. It has become a $100 billion industry in 2021, and that figure is expected to more than double by 2024.

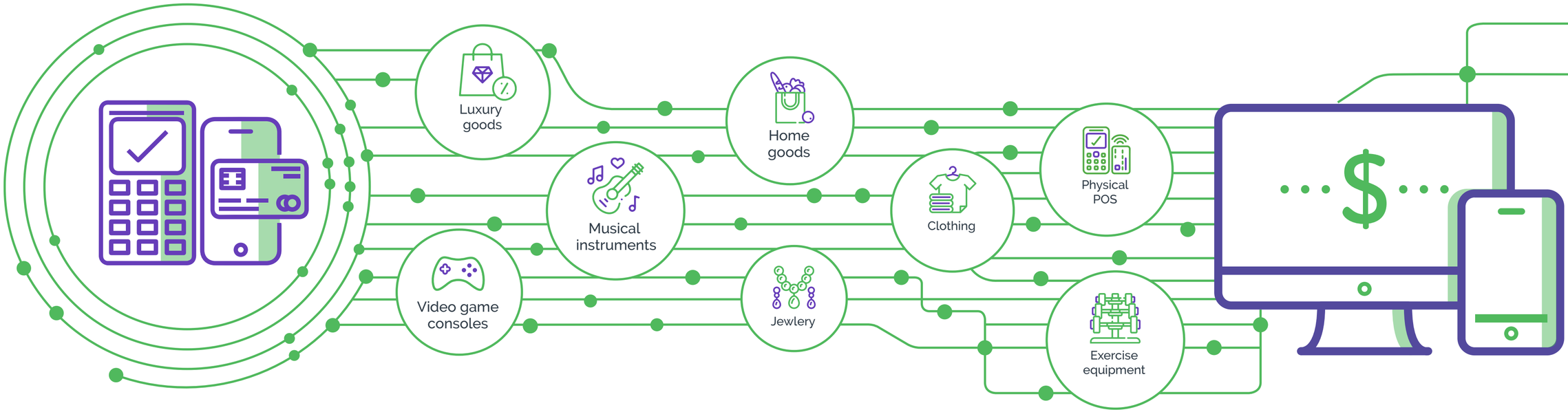
BNPL became especially popular during the pandemic. Customers facing economic uncertainty were able to buy products and services immediately without bearing the burden of making full payment at the time of purchase. It provides consumers with a handy method to tide over temporary financial setbacks, and can help them rebuild their credit after financial hardship.

Of course where there is lots of money, there will be attackers. BNPL fraud is fueled by the massive amount of personal data that has been exposed through years of data breaches. In the BNPL model, customers can secure approval for a loan in seconds and receive purchases having paid either nothing or a minimal amount upfront. By utilizing synthetic identities, attackers exploit this model with no intention of paying back the loan amount.

An Explosion Of Buy Now Pay Later Adoption

The evolving fintech landscape provides innovative and user-focused alternatives to legacy lending options. That is evident in the explosion of digital BNPL services that have popped up over the last 18 months or so. Consumers rely on BNPL to purchase goods in a wide range of industries, and it is a truly compelling proposition for consumers and merchants alike. Merchants see it as a powerful way to attract and retain highly-engaged consumers; and for BNPL users it is a simple and accessible way to access credit, with a fraction of the fees and interest rates that traditional credit options would offer.

BNPL has also enabled increased financial inclusion, offering those outside the traditional financial ecosystem access to credit. It enables individuals who can't access traditional credit lines to easily buy items on credit. It also benefits younger people on lower salaries and students who want access to the latest goods and services, without racking up costly credit card debts.



Top 4 Threats To Buy Now Pay Later Platforms

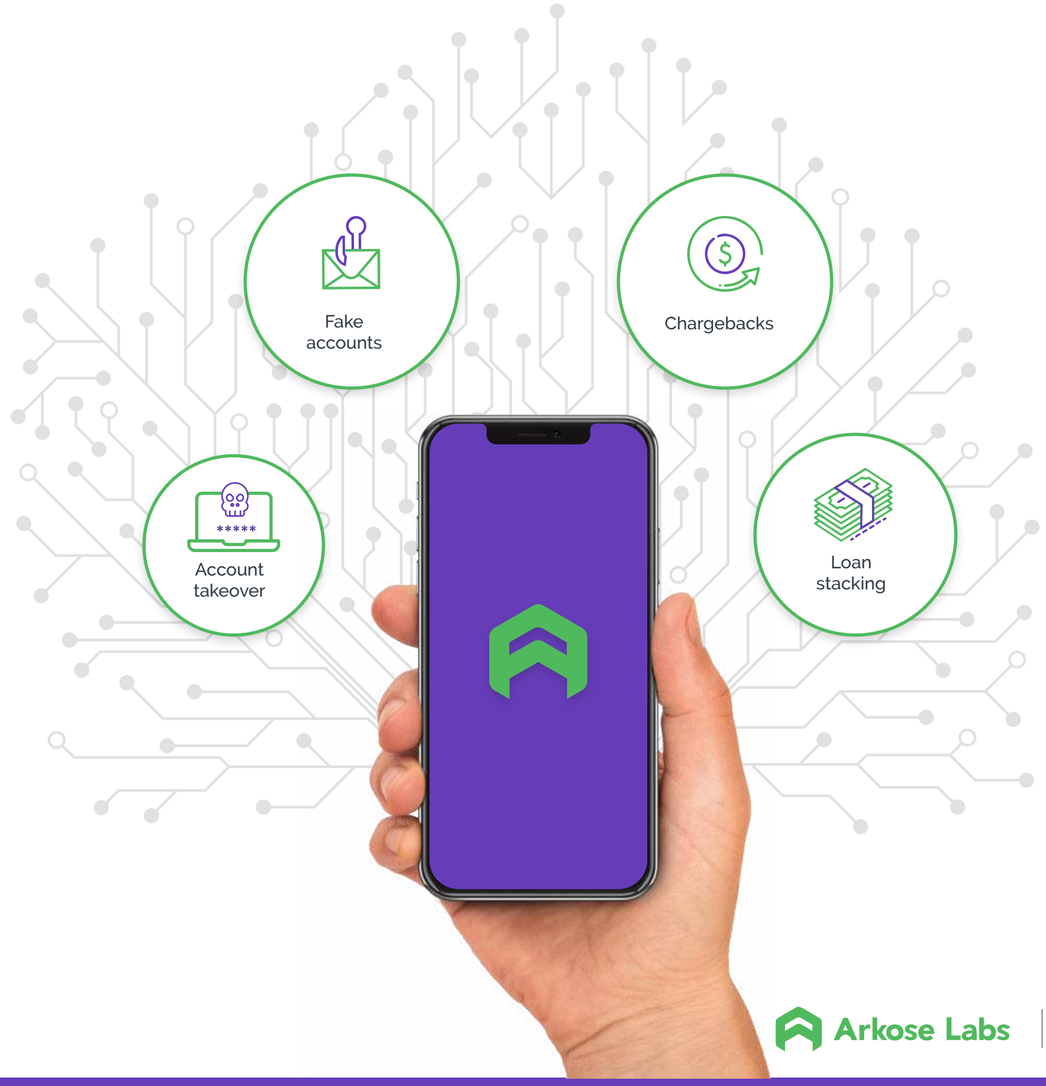
The rise in popularity of BNPL platforms makes them a juicy target for malicious activity. Providers can expect the same sort of attacks that the merchant ecosystem has been seeing for years, but the nature of this novel business model means that attackers will be more highly motivated, as there is a clear route to monetization. Organized fraud and cyberattack operations will be focusing on ways to scale up attacks across the various BNPL platforms which have come to market.

- **Account Takeover -** Bad actors seek to compromise trusted user accounts to carry out transactions using credit cards details on that account and steal items. Account takeovers are carried out by both bot attacks and organized human attackers.

- **Fake Accounts -** The risk of identity fraud at the account sign-up stage is high on BNPL platforms. Attackers purchase stolen and synthetic identities on the black market and carry out scripted account creations to set up attacks and carry out fraud and cyberattacks.

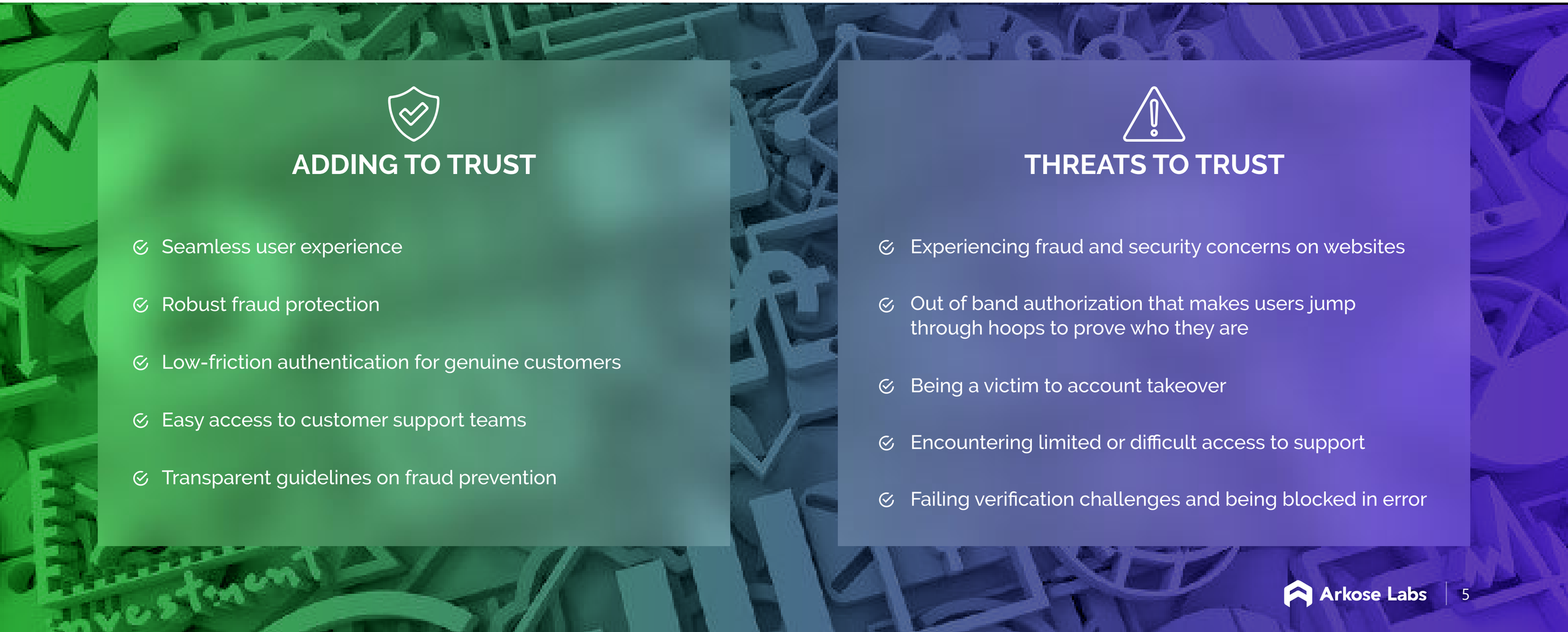
- **First-party fraud -** BNPL platforms are very susceptible to "friendly fraud", with individual users abusing the system to avoid paying the installments after they have their item or claiming it was not them.

- **Loan Stacking -** With the increase in the range of BNPL providers which are now plugged into merchant sites, there is a risk of a new flavor of loan stacking, whereby bad actors carry out transactions across the multiple providers with no intention of paying the installments.



Building And Preserving Trust In Buy Now Pay Later

BNPL platforms are known for their optimal user experience, but these must be balanced with proper fraud and security controls. Experiencing fraud or too much friction will lead to a decrease in trust. As consumers sign up to new services and make transactions on these emerging platforms, every interaction they have goes to either build or erode trust.



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 and security concerns on websites
- 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

The High Stakes Game Of Account Takeover

Accessing financial accounts through account takeover allows attackers 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

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

Additionally, as fraud and security technology evolves, criminals are increasingly employing cheap human labor in developing economies to turbo-charge attacks. Arkose Labs found that human-driven attacks increased steadily throughout 2021.

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

Five Key Steps To Tackle Buy Now Pay Later Fraud

With BNPL platforms juggling a mixture of fraud, security and credit risks, we will look at the top ways, they can protect themselves against organized attacks on their platforms.

Fraud and security teams at digital-born companies have an opportunity to bake security into their products from the outset. They are not operating on legacy IT systems and dealing with internal siloes, in the way that traditional businesses going through digital transformation are. BNPL companies must prioritize future-proof strategies that protect the integrity of their platforms, while scaling with rapid growth.

BNPL platforms have the twin challenge of fighting rising attack levels, while still maintaining a seamless customer experience. Some businesses take the mentality of allowing a certain level of fraud to exist -- seen as a "cost of doing business" -- but this only perpetuates the cycle of cybercrime and encourages future attacks. Due to the negative consequences of any breakdown in trust on BNPL platforms, businesses need a zero-tolerance approach to which defeats the long-term drivers of attacks.

Step 1

Real-Time Risk Decisioning

Empower your decisioning with AI-powered risk analysis and actionable data insights.

Buy now pay later platforms need a defense-in-depth approach to detecting malicious activity on their platforms as early as possible. They must analyze risk signals across consumer touchpoints in real-time including device, network data, location and behavioral biometrics. In a fast-evolving threat landscape, attackers will go to great lengths to spoof or obfuscate signals in order to blend in with legitimate traffic and evade known detection techniques. Businesses therefore need to constantly tune attack signatures, using machine learning for historical attack calibration and anomaly detection, as well as human analysis of traffic patterns.

The optimal solution should provide:

- Real-time analysis of risk signals across device, network, and location
- Machine learning models for traffic forecasting and anomaly detection
- Behavioral biometrics to distinguish trusted versus malicious patterns
- Actionable risk insights that provide a clear route to remediation for high-risk traffic

Step 2

User-Friendly Interdiction Of High-Risk Traffic

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

BNPL providers need maximum protection of their sign-up, login and transaction points, and security challenges can be a powerful way to eliminate a great deal of organized, malicious activity by introducing friction specifically targeting attackers. Due to the nature of the business they need to achieve this in a fully user-centric way with minimal intervention rates for good consumers. When reserved for riskier traffic, and using methods which are easy for legitimate individuals to complete, friction can be a positive security measure that helps preserve trust and demonstrate that steps are being taken to protect users' accounts against online abuse.

Key components of intelligent friction:

- Deploy in-session step-up challenges which are tailored to the risk profile
- Invest in a risk engine that can keep interdiction rates to as low as 1% of good users
- Develop anti-automation challenges that use interactivity and logic to defeat bots, and are tested against the latest machine learning solving techniques
- Target human attackers with more complex challenges that analyze behavior and frustrate organized fraud operations

Step 3

Shift The Attack Surface

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

BNPL providers need to shift the attack surface away from their digital frontline and leverage specialized third parties to keep attacks at bay. Independent verification of user activity avoids draining in-house fraud and security resources and provides a buffer between the attackers and the sites they are so practiced in attacking. By working with external vendors, it also sets BNPL security and fraud teams up for any major spikes in activity - including a surge in good user activity as the platform grows its user base or goes through seasonal shopping spikes; or when they experience a sustained, targeted attack from an organized cybercrime organization.

Benefits of shifting the attack surface:

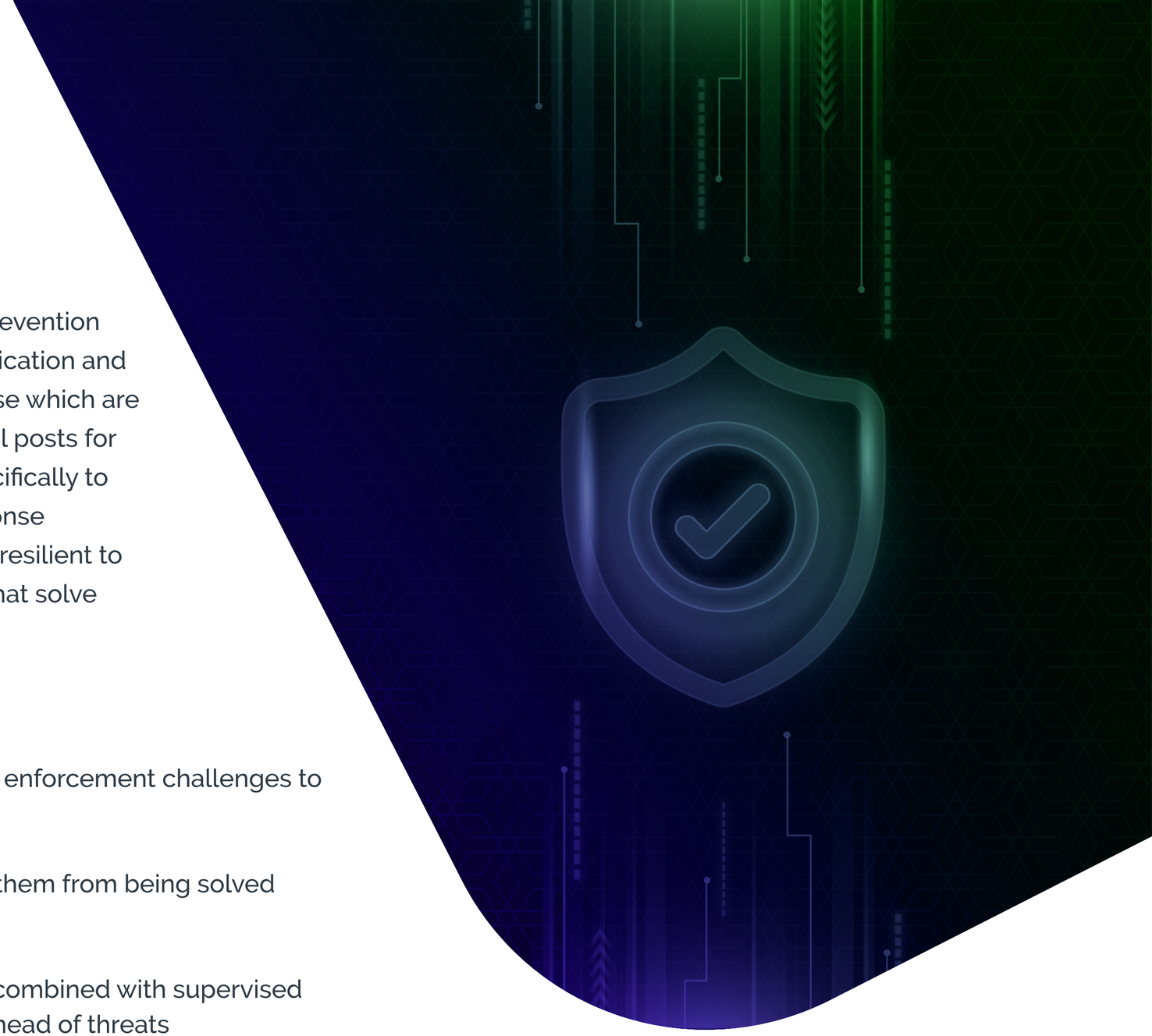
- Attackers have to get through intermediary security steps rather than directly attacking BNPL touchpoints
- The projected attack route is disrupted, hampering attackers ability to execute as planned
- Businesses avoid the need to divert their internal resources to deal with spikes in attacks

Step 4

Adapt To Evolving Attacks

Stay ahead of cybercrime with future-proof protection.

Attackers have learned to circumnavigate data-driven fraud prevention systems, and use automation to bypass many step-up authentication and security controls at scale. The most effective defenses are those which are by-design constantly evolving in order to keep moving the goal posts for attackers. For example, Arkose Labs' platform is designed specifically to detect device and credential spoofing, and its challenge-response technology is continuously changing and tested to ensure it is resilient to being circumvented by the latest machine learning methods that solve challenges at scale.



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
- Orchestration platforms with embedded machine learning combined with supervised models which security analysts monitor and tune to keep ahead of threats

Step 5

Invest Strategically To Keep The Fraud And Security Technology Stack Simple

Safeguard the key advantage of nimble fintechs by keeping fraud and security costs and complexity to a minimum. Traditional banks have convuluted 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 and BNPL providers have a distinct advantage: they are able to implement streamlined fraud and security 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, fintechs need to balance innovative technologies with a strong commitment to successful outcomes:

- Real-time intelligence
- Protection across multiple use cases
- Committed customer success team
- Simplified integration and deployment
- Intelligent friction
- Ability to defeat multiple attack vectors
- Innovative technology and machine learning
- Rapid time-to-value

A Digital-Born Fraud And Security Solution For Buy Now Pay Later Providers

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.

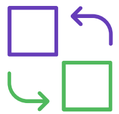
Arkose Labs' platform is tailor-made for companies looking to deliver a standout user experience, while retaining a zero-tolerance approach towards attacks on consumer accounts. It is the only platform to seamlessly combine risk-based and step- up authentication, with a continuous feedback loop which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

In a world where digital identities have been corrupted and attackers have access to highly sophisticated tools, Arkose Labs is combatting the growing online fraud and security 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 attackers on the other hand, these challenges eliminate all automated attacks and prevent human-driven attacks from scaling.

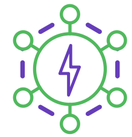
The Arkose Advantage

Arkose Labs has been designed to combat fraud in the post-breach era. Its AI-powered platform combines real-time risk assessment with dynamic attack response to defeat persistent bots and co-ordinated human attacks on the most targeted user action points on BNPL platforms. Invisible risk assessments allow good users to pass through seamlessly. High-risk traffic is triaged for active attack response that deters future attempts and creates a more secure experience for genuine customers. By significantly increasing the labor involved in clearing challenges it breaks the business model behind organized fraud. Arkose Labs' multi-step defenses work together seamlessly, and create a continuous feedback loop to ensure BNPL platforms stay ahead of evolving threats long term.



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

Protects Against Automated Attacks
Robust anti-automation provides a commercial guarantee against all automated attacks.



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, 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 attackers from bypassing its platform at scale using automation or fraud farms.

Arkose Labs

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.

Offices

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

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

United Kingdom
167-169 Great Portland Street, 5th
Floor, London, W1W 5PF

Schedule Demo