Arkose Labs | SOLUTION BRIEF

Buy Now Pay Later Fraud

Account Security and Fraud Prevention

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. Naturally, that has caught the attention of fraudsters and bad actors.

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.

Since the upfront payment amounts are lower, consumers choosing to pay using BNPL, usually have a greater propensity to buy more items. This benefits merchants in the form of larger basket sizes, improved conversion rates, and lower cart abandonment rates. Furthermore, the convenience of BNPL services help build customer loyalty, which can result in repeat business for the merchants.

Buy Now Pay Later Becoming a Top Target for Fraud

Of course where there is lots of money, can the fraudsters be far behind? Bad actors are increasingly targeting BNPL platforms due to the high potential to make significant amounts of money with attacks. This 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 stolen and synthetic identities, fraudsters exploit this service with no intention of paying back the loan amount. In addition to using synthetic identities to create new accounts with the intention of committing fraud, attackers also target existing accounts with credential stuffing attacks.

Negative Effects of Increased Attacks on Buy Now Pay Later Companies:

- **Chargebacks:** If a real customer is the victim of an ATO attack, the BNPL provider then has to issue a chargeback.
- **Lost Revenue:** BNPL firms extend loans to fraudsters using synthetic identities who have no intention of paying them back.
- **Unwanted Friction:** Fighting rising fraud attacks with cumbersome authentication protocols hinders the seamless BNPL experience.
- **Brand Reputation:** Customers whose accounts get hacked will move to competitor platforms and complain on social media.

[1] www.cnbc.com/2021/09/21/how-buy-now-pay-later-became-a-100-billion-industry.html

Account Security and Fraud Deterrence

The rising popularity of BNPL and the ease of transactions have caught the eyes of the fraudsters, who are using the convenience to make money for themselves. They take advantage of the fact that BNPL providers only have a few seconds to approve or reject a purchase to escape with expensive items at a minimal cost – often paid using stolen credit cards – making it harder for deserving customers to leverage the services.

Common Attack Techniques:

Account takeover: A user account with a good repayment record enjoys greater lending limits and is more attractive to fraudsters. Attackers use several tactics, including credential stuffing and automated phishing, for account takeover to exploit compromised accounts.

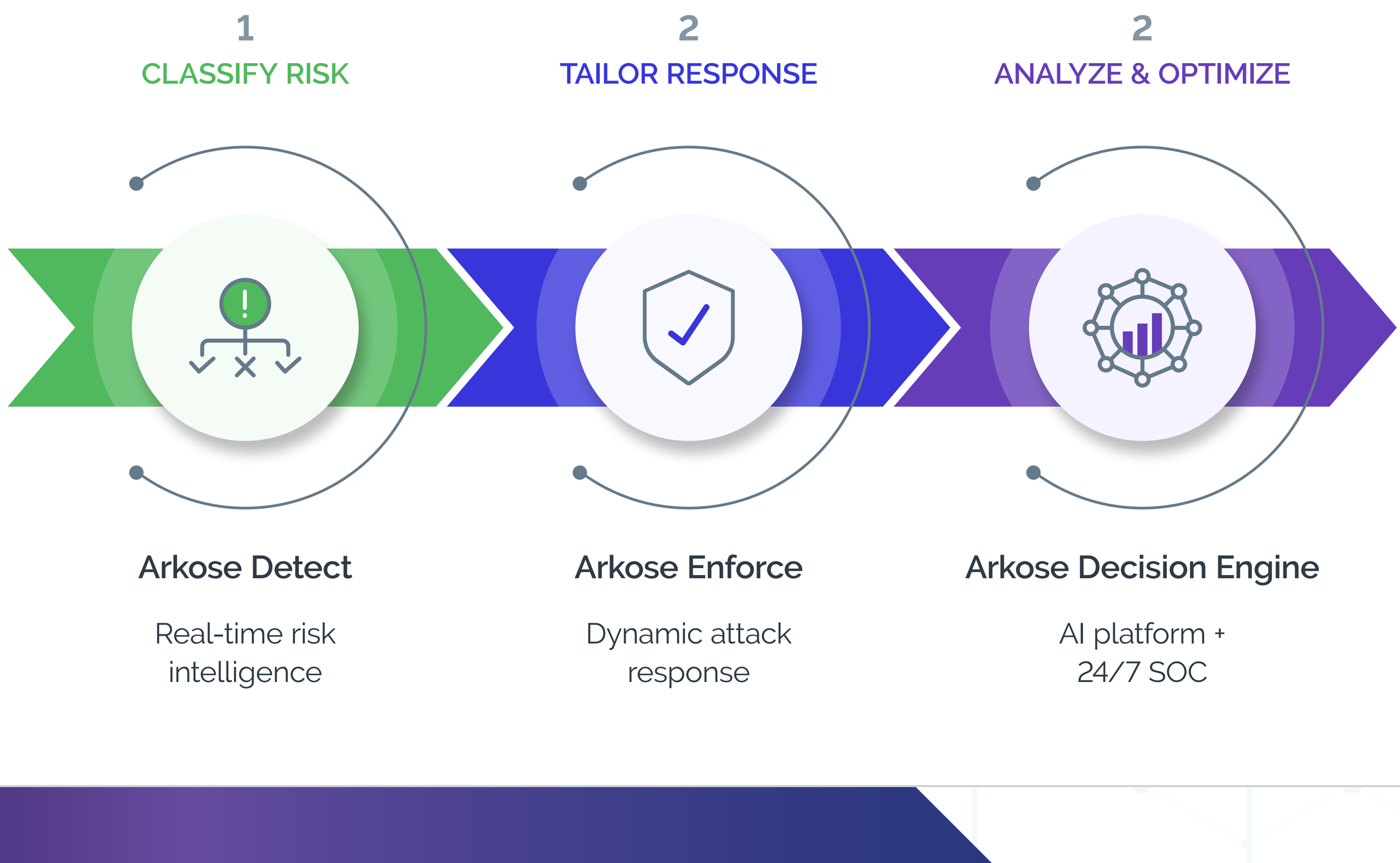
New account creation: Fraudsters use synthetic or stolen identities and create fake new accounts, using bots to scale up attacks. Fraudsters use these fake accounts to make multiple purchases using stolen credit card deta, leading to chargebacks and settlement costs.

Bypass authentication methods: Attackers will bypass authentication steps at scale, and try to orchestrate their activities with the least resistance. Businesses need powerful protection at the account sign-up and login steps to detect suspicious actors early - all without threatening the seamless user experience.

The Arkose Labs Approach

Identities are being spoofed at scale and traditional authentication steps are being circumvented. That's why Arkose Labs combines rich data intelligence with powerful analytics to discern intent, and proactively fight spoofed identities and devices. Its AI-powered platform evaluates fraud patterns across different websites and apps, and then ensures the correct tools are in place to flag risky users in real-time.

This intent-based approach means that the vast majority of good users continue to have a seamless experience, while targeted friction frustrates human fraudsters and stymies bots.



Arkose Labs Protects Buy Now Pay Later Platforms

Arkose Labs carries out deep analysis of behavior, device and network heuristics to segment suspicious activity for the appropriate attack response. Businesses receive actionable telemetry to inform further actions, and Arkose data can be used to train businesses' internal models, including attack signatures, reasons for risk classification, fingerprint information, and more.

Arkose Labs also provides businesses with dynamic attack response, to go beyond a risk classification and actively remediate fraud attempts. Its innovative in-band enforcement challenges provide powerful secondary screening of high-risk traffic, in a way that does not disrupt legitimate users.

This tackles abuse in real-time. Even the most advanced bots are thwarted with interactive challenges. Malicious humans are shown increasingly complex challenges until they give up in frustration and leave. This is achieved while maintaining a completely user-centric approach to security that challenges suspicious traffic using incremental risk-based friction, rather than blocking it outright.

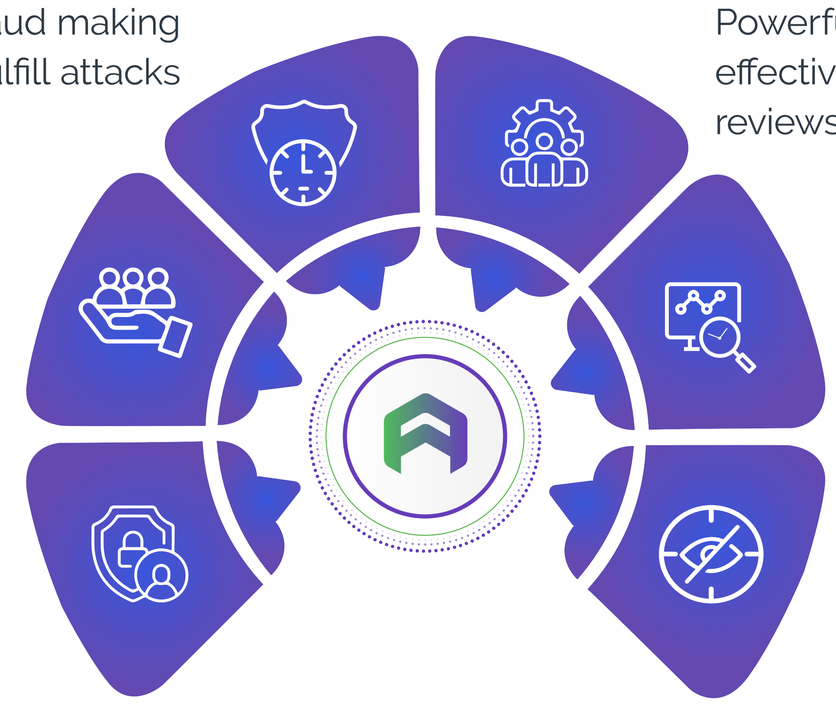
Arkose Labs works with companies across the globe to fight all attacks across the digital frontend including account takeovers, credential stuffing, fake new account fraud, spam, phishing, scraping, inventory hoarding and more. Arkose Labs helps BNPL platforms to continue to deliver a seamless user-centric experience to customers while keeping fraudsters out of your ecosystem.

The Arkose Advantage

Long-term deterrence
Arkose Labs increases the cost of fraud making it economically unsustainable to fulfill attacks

Effortless management
Powerful decision engine selects the most effective response strategy to reduce manual reviews

Protection across the customer journey
One flexible solution that protects against different attack vectors and extensive user touchpoints



Early detection
Eliminate losses, reduce costs, and streamline efforts by preventing attacks before they advance in your ecosystem

Privacy friendly
Arkose Lab technology achieves unparalleled accuracy without compromising data protection compliance

Results fast
New customers will see results within days, not weeks or months.

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.

Email:
demo@arkoselabs.com

Schedule Demo