Ebook

Arkose Labs

8 Trends Fueling Account Takeover Attacks on Banks

How banks can combat the biggest threat in fraud

The Rising Storm of Account Takeover Attacks

Banks have always been among the most popular targets for criminals. Whereas in years past they would risk life and limb by holding up branches with firearms, today's fraudster can gain access to any number of bank accounts from the comfort of his or her own home. It's no stretch to say that account takeover attacks are one of the greatest threats facing banks today. Massive and frequent data breaches over the years have exposed millions of records containing personal information that fraudsters can easily obtain. They use this stolen PII to launch a bombardment of attacks against banks.

In 2018, account takeover attacks caused $4 billion in losses for the economy overall, while 80%-90% of the fraudulent ATO logins are carried out by automated bots. Clearly, this is a very popular attack vector for cybercriminals of all stripes. [1] Further, according to Arkose Labs data, there was a 17% increase in account takeover attempts recorded on our platform at the beginning of 2020.

With the rise in popularity of mobile banking, attackers are increasingly focusing their efforts here. In fact, finance has the highest amount of mobile engagement of any industry on the Arkose Labs network, with around half of all financial transactions originating from mobile devices.

[1] *https://securityboulevard.com/2019/06/the-costs-and-risks-of-account-takeover/*

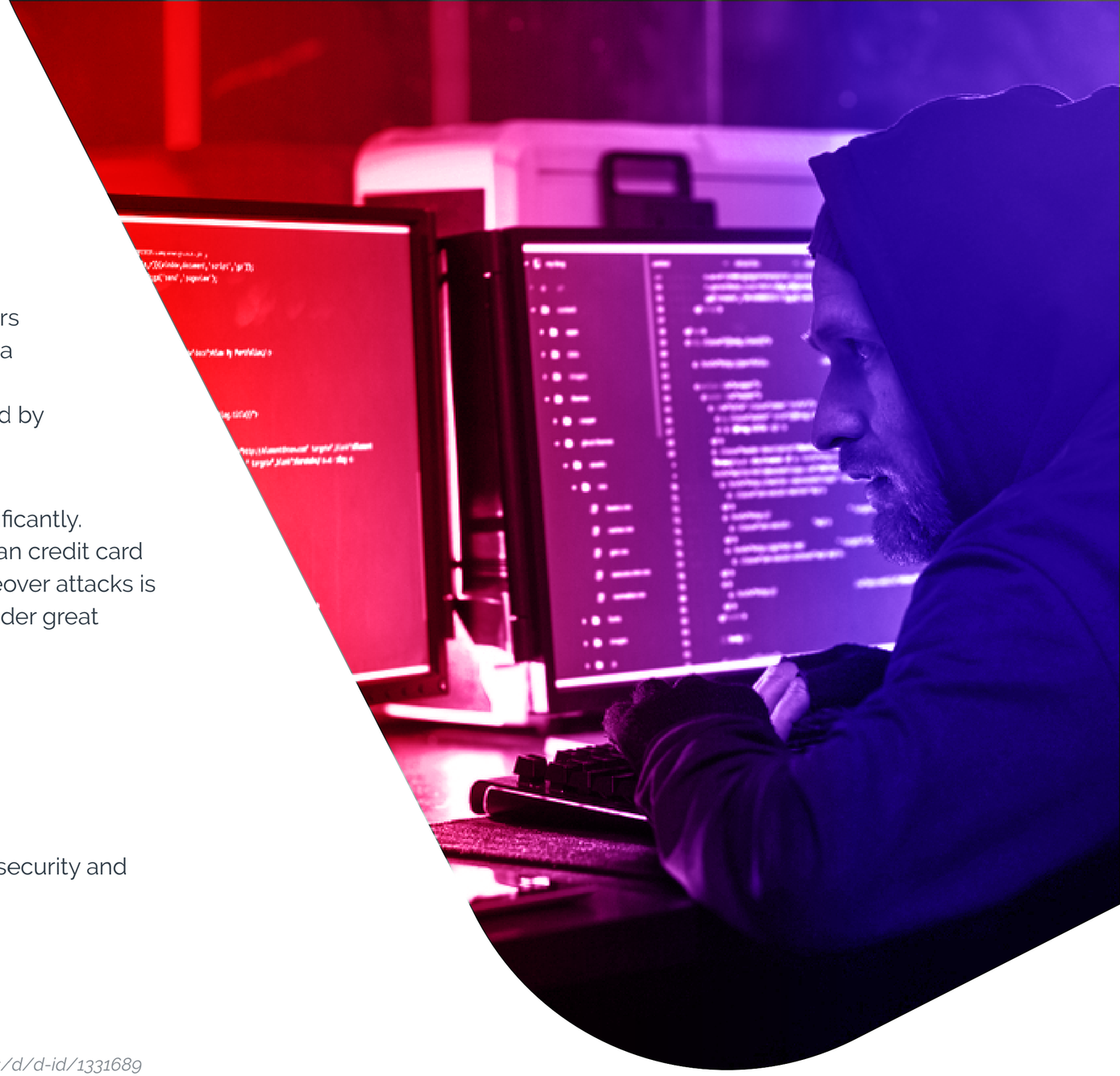
1 Banks are Targeted by Organized Cybercrime and Fraud Ecosystem

ATO attacks on bank accounts are a crucial part of the wider ecrime ecosystem. Incentive levels are high, so the opponent is highly motivated and driven by financial return. Attackers will leverage "services" ranging from identity farms and malicious coders to obtain the personal data and tools required to launch large-scale attacks. Once bank accounts have been accessed, it is not just the initial act of stealing funds from that account which motivates them. Accessing financial accounts allows fraudsters to commit a range of cybercrimes, with very serious consequences for individual users, banks' profits and wider society.

2 Identity Data has been Corrupted at Scale

We live in a world where digital identities have been corrupted, and stolen credentials can be accessed by attackers with minimal effort or expense. Users cannot be relied upon for responsible password management - according to a survey by Dark Reading, 59% of people reuse passwords despite 91% of respondents acknowledging the associated risks. [1] Other PII can be purchased by cyber criminals for as little as a dollar on the Dark Web.

As a result, account takeover attacks using stolen identity data are rising significantly. Identity information has become a more valuable commodity for attackers than credit card information as the long-term payout for using this information in account takeover attacks is higher. Financial institutions cannot trust digital identities anymore and are under great pressure to protect user accounts.



Financial Fraud at a Glance

01 $4 billion lost by banks in ATO attacks in 2018[2]

02 2 out of 5 consumers have closed a financial services account due to security and fraud concerns

03 Account takeover attacks peak in the evening for banks

[1]https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689

[2]https://www.pymnts.com/news/digital-banking/2019/us-bank-machine-learning-is-banks-best-bet-against-fraud/

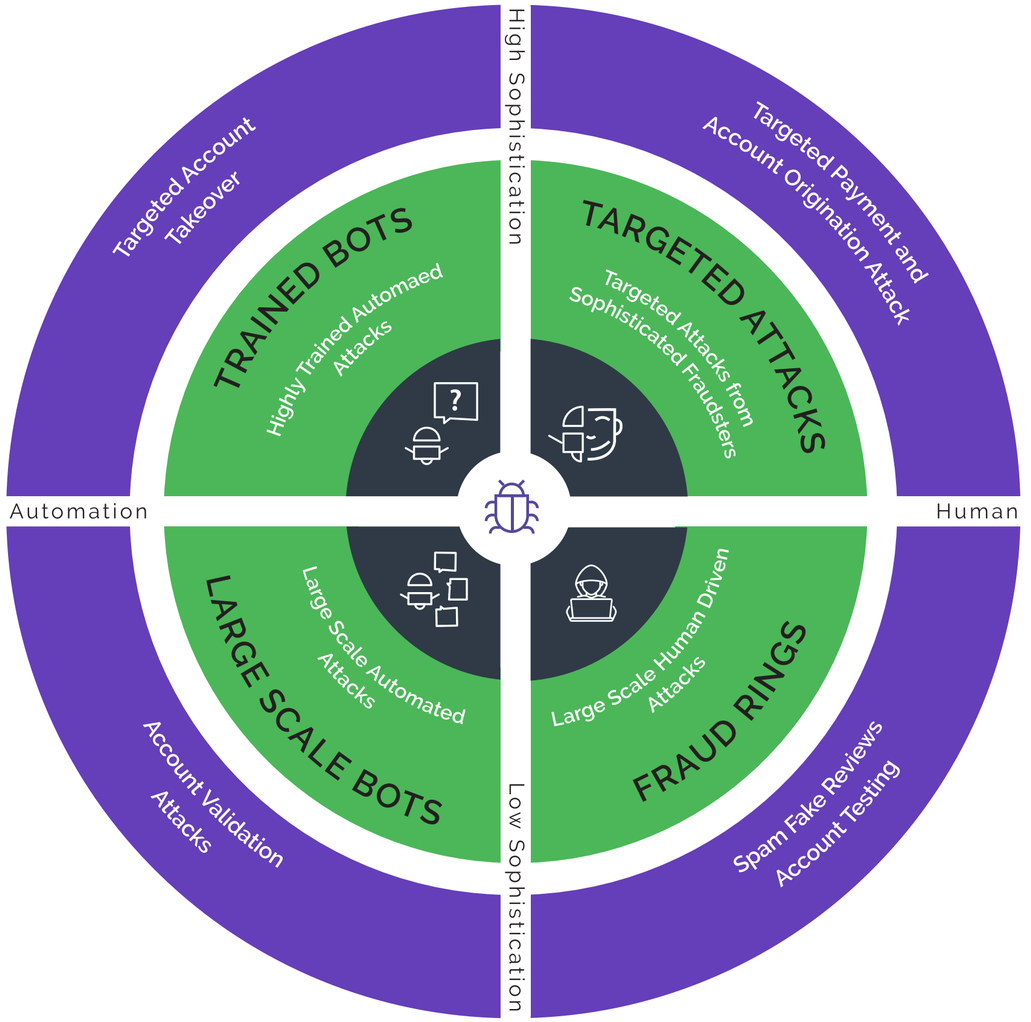
3 Digital Banking Faces Multi-Pronged Attack Tactics

Banks need to protect their digital front-end from an array of attacks of different sophistication levels. Attackers have honed their craft and are constantly testing enterprise defenses. Automated attacks are on the rise, and many of these bots are advanced to the point of accurately mimicking human behavior online. Advances in machine learning and machine vision mean that malicious bots can bypass and overwhelm the mitigation software being used today.

Attackers also deploy large-scale fraud farms - teams of human workers who are paid by the login attempt hack into accounts at scale. These human workers can easily bypass legacy challenge-response solutions which are designed to protect purely against automation.

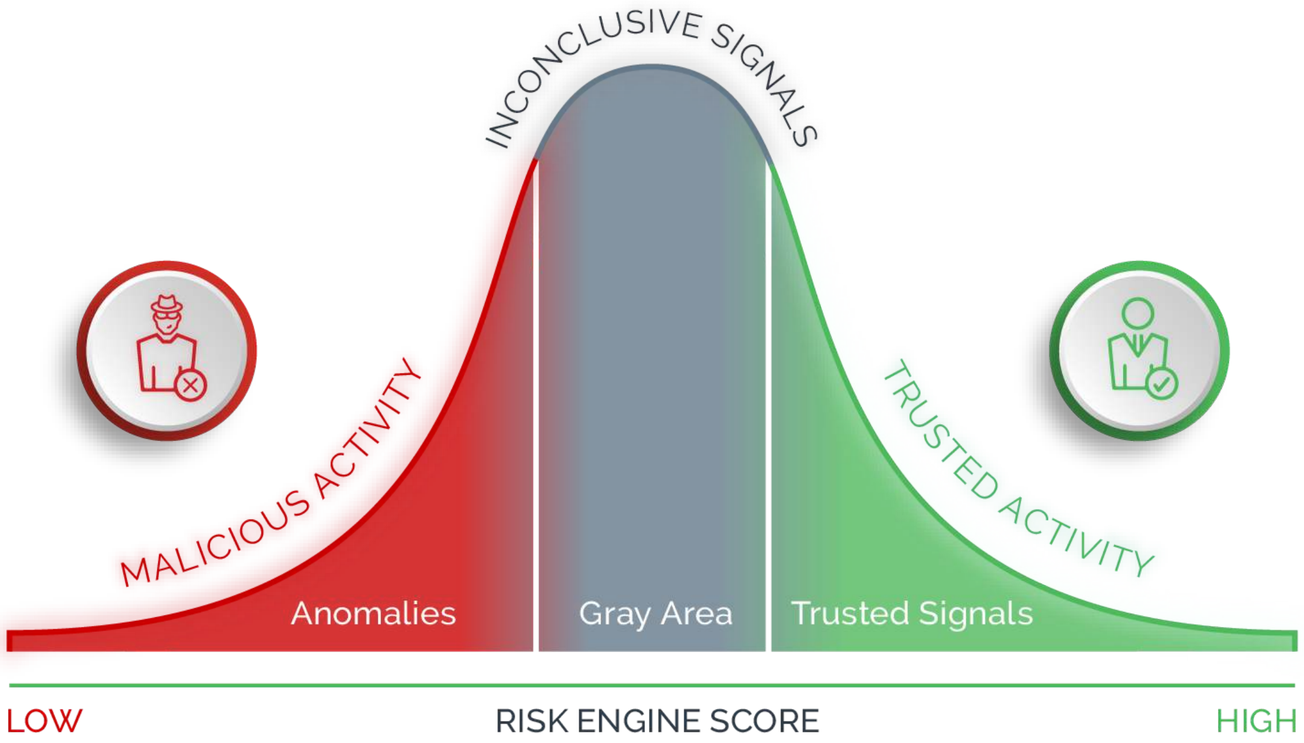
Banks are facing great complexity and coordination on the part of attackers, who have more powerful tools and know-how than ever before. Defending against such attacks is made even more difficult because of the massive amount of data banks must ingest and analyze on a daily basis.

Banks also must navigate this increasingly hostile threat landscape without placing overly stringent controls during the login process. It's a fine line between fighting fraud and alienating customers.



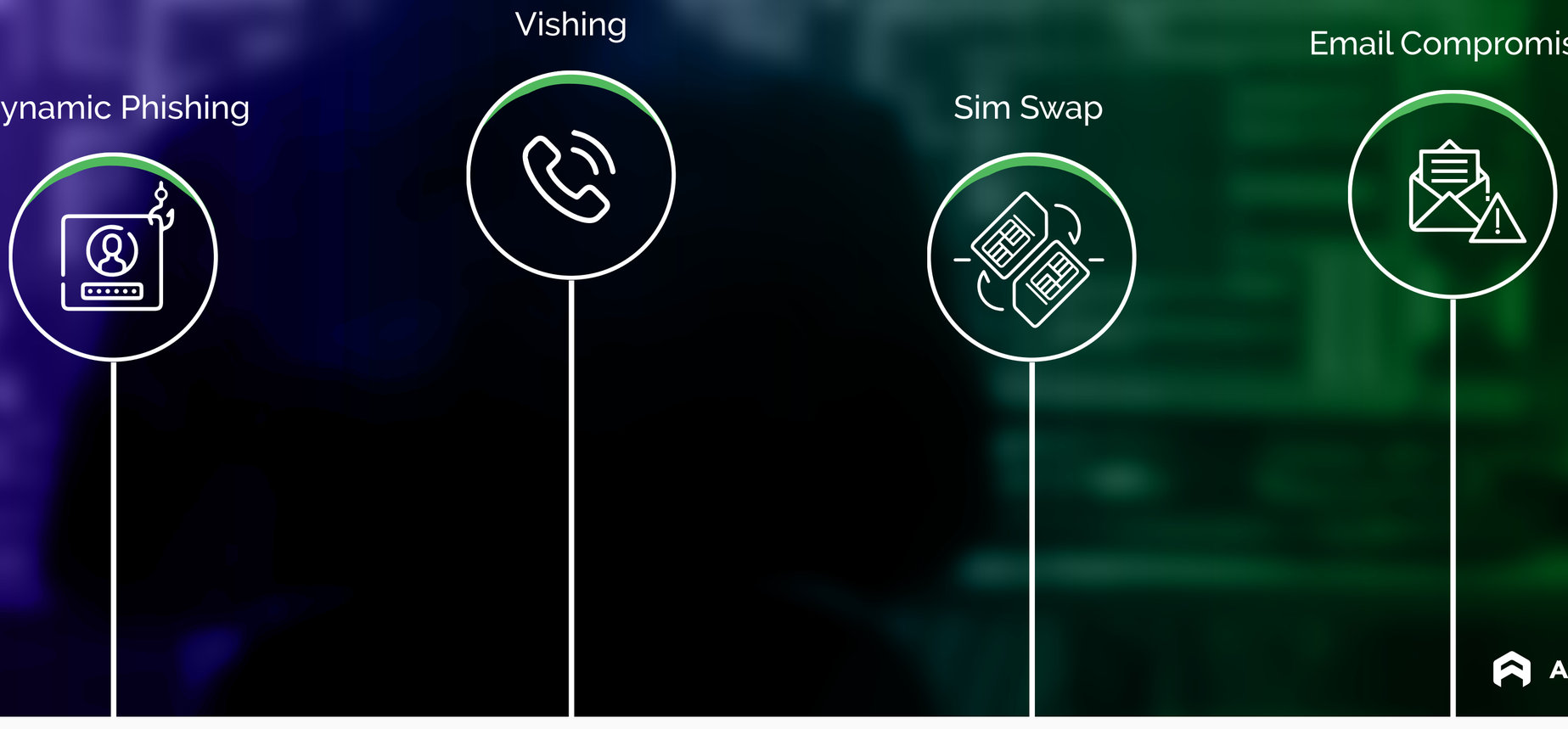
4 Risk Signals at Logins are Increasingly Inconclusive

Fraudsters have become adept at mimicking “good” user behavior and spoofing devices and identities in order to attempt to evade fraud and security detection capabilities. Despite extensive investments in talent and technologies by banks, it is increasingly difficult to action fraud prevention insights with confidence. While on some occasions there are clear data signals or digital identifiers that mark out traffic as clearly “good” or “bad”, this is often not the case. More and more traffic seen by businesses today falls under a “gray area” in between. Banks need layered detection capabilities, which are tailor-made for a world in which attackers are spoofing signals at scale. They also need to perform secondary screening on segments of high-risk traffic for more definitive risk classifications and embed a continuous feedback loop of truth data into decision engines.



5 Attackers are Evading Multi-Factor Authentication to Carry Out ATO

Attackers have many different ways to compromise accounts and evade known defenses such as multi-factor authentication (MFA). Advanced automated phishing has evolved to capture one-time passwords and SMS tokens alongside user credentials on a fake site, and leverage this information in real time to hack into the legitimate site while the token is still valid. These attacks rely on trained bots to dynamically orchestrate these attacks. This shows that even when logins are protected by MFA, sophisticated profiling of traffic for signs of advanced bots is a necessity. Sim swap attacks, social engineering and vishing attacks via phone calls will also aim to circumvent this layer of defense, further highlighting that out of band authentication is no silver bullet for account security. Attackers have a wide range of techniques they use to achieve their goal and are very persistent.



6 UX Improvements at Login are Exploited by Attackers

Customers not only expect that their bank will keep their digital transactions secure, but they also want a quick and easy authentication experience. According to a Bain & Co. study, customers who are satisfied with their bank's digital capabilities are more loyal and tend to be more valuable customers on average.[1]

But many of the authentication methods commonly in use create for a bad customer experience. Two-factor authentication via SMS codes are an annoyance for customers and don't always have wide adoption rates. There are also increasing ways for attackers to circumvent multi-factor authentication.

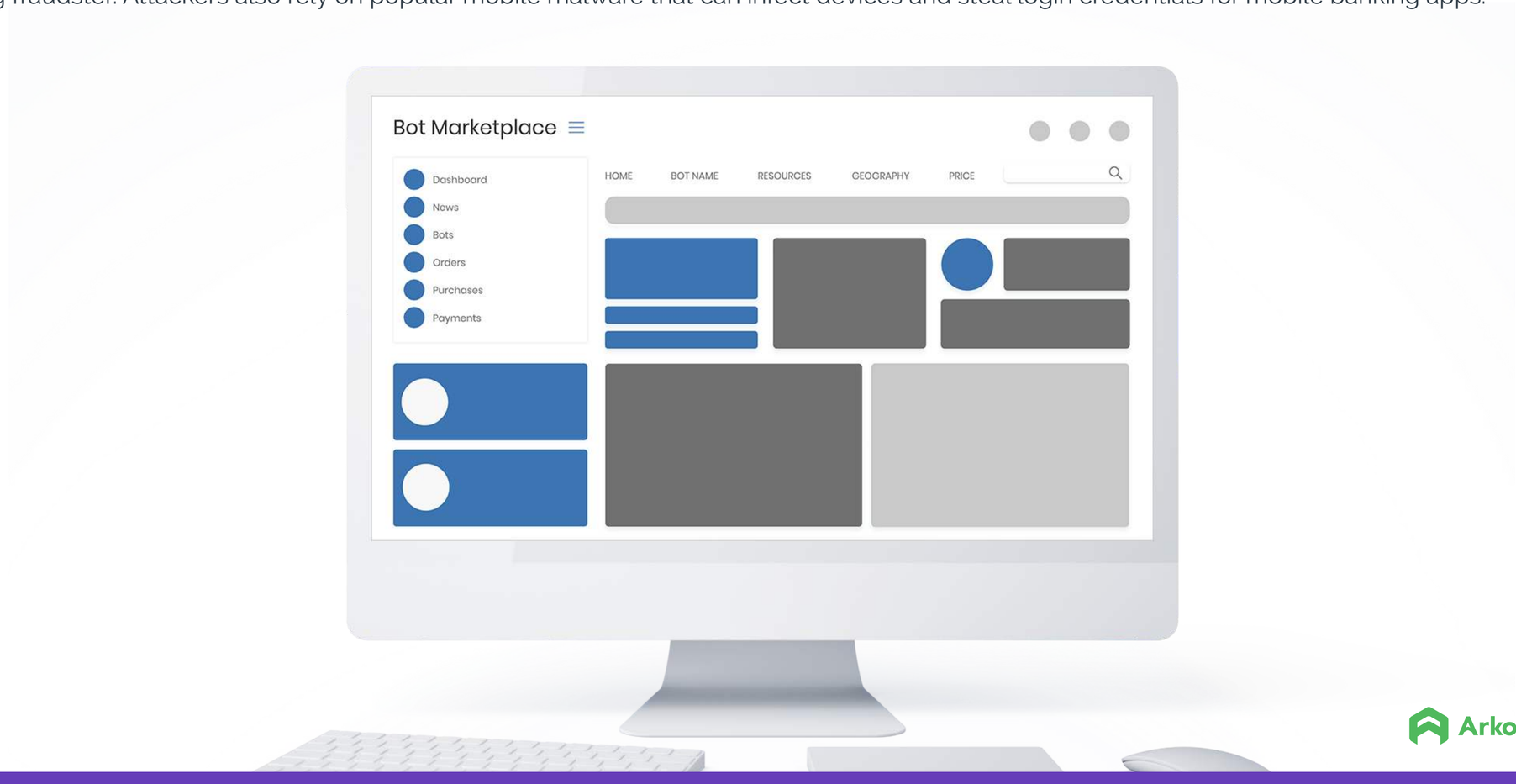
Knowledge-based authentication methods are also just as ineffective. For one, many customers fail them, as they often forget their best friend's name from the first grade or make and model of first car. And this information is easily obtainable for fraudsters, either through stolen data or even via basic web searches or from scraping social media profiles.

[1] *https://www.bain.com/insights/as-retail-banks-leak-value-heres-how-they-can-stop-it/*

7 Credential Stuffing Provides a Simple Way to Attack Accounts at Scale

Credential stuffing is still widely used to hack into accounts. More sophisticated credential stuffing techniques have developed to bypass traditional bot defenses, using headless browsers and enabling bots to execute JavaScript and mimic human activity, while keeping volumes low enough to avoid triggering rate limiting rules.

Due to the organized shadow cybercrime marketplace, these tools are easy to access and very simple to use. This means the person carrying out the attack on a bank does not need advanced technical knowledge to run credential stuffing attacks, and the barrier to entry is low. Tools are obtained on the Dark Web and YouTube videos even show attackers step-by-step how to set them in motion. Like legitimate businesses, these sites even offer "premium" services with on-demand customer service for the truly enterprising fraudster. Attackers also rely on popular mobile malware that can infect devices and steal login credentials for mobile banking apps.



8 Consumers and Regulators Will Blame Banks

Every successful banking ATO attack erodes customer trust, causes financial loss, and has negative consequences for the economy as a whole. Banks help power the online economy and facilitate the digital movement of money. As a result, both consumers and regulators hold banks to far higher standards than other industries with regards to security. Ultimately, banks will be blamed for any breach, even though they are the victim of a crime.

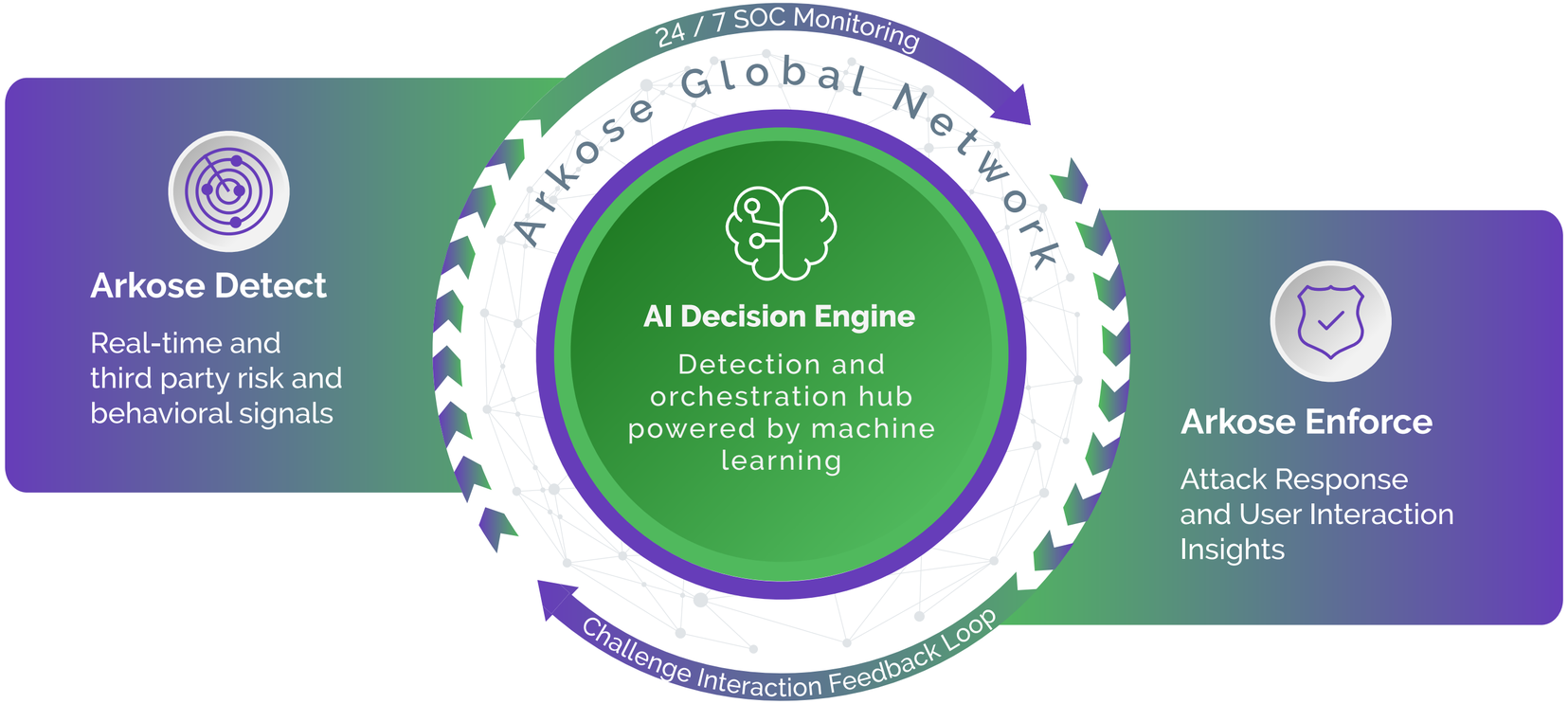
Banks can be subject to dozens of federal and state regulating agencies and numerous complicated and lengthy regulations such as Dodd Frank, the Bank Secrecy Act, Gramm-Leach-Billey, the PATRIOT Act and many others. They face constant regulatory scrutiny and potential fines that could reach into the billions of dollars.

The Waterfall Effects of ATO Fraud

Arkose Labs: A New Way to Tackle ATO for Banks

Global banks trust Arkose Labs to detect and deter attacks at user authentication touchpoints where account takeovers, credential stuffing, and fake account creation attacks originate. By rooting out fraud early, companies are able to strengthen relationships with customers by offering an increasingly secure financial platform without sacrificing a positive user experience.

Arkose Labs delivers long-term account protection by undermining the economic drivers behind attacks. Our AI-powered platform defeats persistent bots and coordinated human attacks on the most targeted user touchpoints on websites and apps. Invisible risk assessments allow good users to pass through seamlessly. High-risk traffic is triaged for active attack response using innovative enforcement challenges that deter future attempts, while delivering a more secure experience for genuine customers.



Banks Need Greater Clarity to Protect Accounts and Enhance UX

When dealing with a growing gray area in fraud detection, banks will often feel compelled to add additional manual checks or out-of-band authentication steps.

Arkose Labs takes a very different approach when dealing with traffic in the gray area. Rather than demanding that a customer jumps through hoops to prove who they are - or expending a great deal of time, effort and resources internally on analysis - it provides a powerful intermediate step which switches the burden from the bank to the attacker.

Traffic is assessed based on real-time risk signals and triaged based on the risk classification. Good users will pass through the Arkose Labs system unchallenged. However, when there are inconclusive signals, banks have the option of presenting a challenge which is simple for an individual user to pass, but is a major roadblock for those looking to attack at scale. This takes away the option of using low-cost automated tools or fraud farms and human resources. This begins to erode their ROI and compel many perpetrators to abandon attacks.

Banks stay in complete control of the challenge strategy and get highly actionable data insights to use in their own models. This gives banks a very powerful new tool in their arsenal, which has far better user experience than MFA technologies.

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.

arkoselabs.com © 2021. All Rights Reserved

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