THE BANKING INDUSTRY AT A CROSSROADS: HARNESSING AI TO FIGHT AI

Key Insights from New Research: The Intersection of AI, Digital Fraud and Cyber Defenses

ARKOSE LABS™

INTRODUCTION

The banking sector stands at the intersection of innovation and vulnerability. With AI transforming the cyber threat landscape, financial institutions face an urgent reality: adapt or risk devastating consequences.

But the path forward isn't clear-cut. Banks must navigate rising attacks, regulatory roadblocks and a critical skills gap. What's at stake isn't just revenue, but the very trust customers place in their institutions.

This infobrief is packed with banking industry insights from our new research, The Intersection of AI, Digital Fraud and Cyber Defenses. It explores how banks can use AI to outsmart evolving threats that typically start at the account level and keep customer trust strong in today's fast-changing digital world.

"The scale of fraud threats and techniques is really escalating, especially with fraud as a service taking off. It's becoming more dangerous every year, and in just a year or two, we could see an exponential spike. That's why we think it's crucial to fight fire with fire. The bad guys are leveraging AI, so we have to be at least as adept, if not better, with our AI defenses."

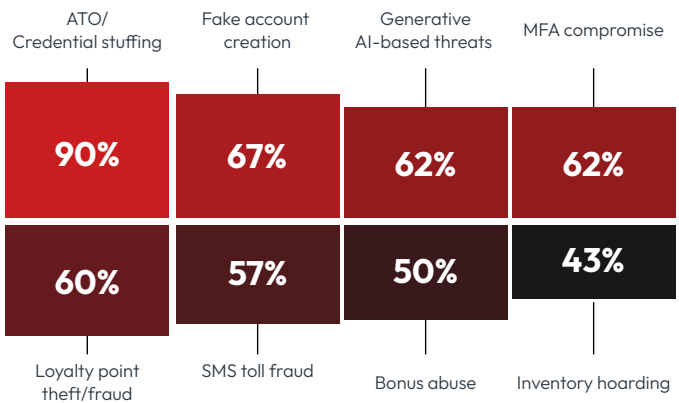
– Senior Executive, Digital Product Management, Financial Services Industry

BANKS UNDER SIEGE

Banks face a wide range of threats to their critical business applications, like websites and apps, with account takeover (ATO) and credential stuffing leading the pack—90% of banks identify these as major risks, far surpassing cross-industry averages of 76%.

But which attack types are seen as the most pressing? Here are the top threats banks believe pose significant risks to their business operations and customers' experience, along with the percentage of institutions concerned to a moderate or large extent.

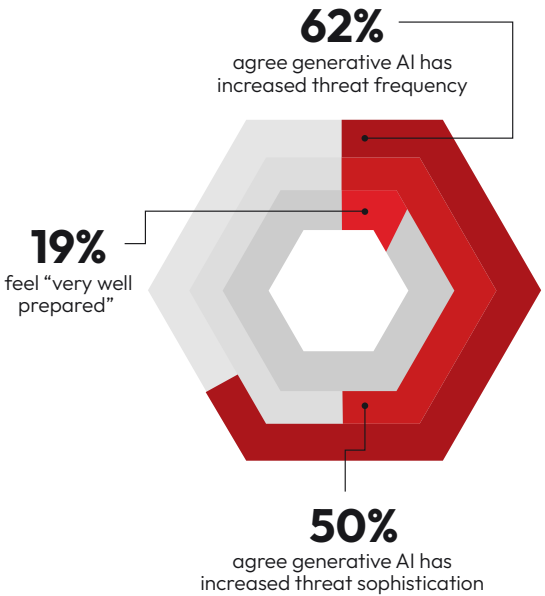
Most Concerning Attack Types



DEFENDING AGAINST AI-POWERED THREATS

Meanwhile, generative AI has amplified the sophistication of these threats, making fraud not only more frequent but harder to detect. The harsh reality is that while cybercriminals are well-prepared to launch AI-powered attacks, most enterprises are playing catch-up.

Yet fewer than one in five of banking respondents consider themselves very well prepared to defend against AI-powered threats. This lack of preparedness is a significant concern, especially when considering the pace at which cybercriminals innovate. Enterprises must close this gap to avoid falling further behind.

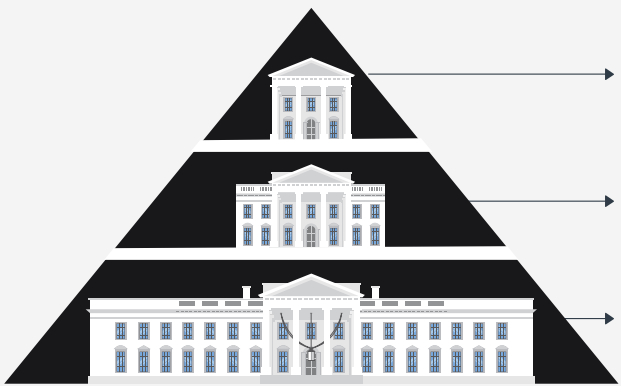


THE BUSINESS COST OF NOT BEING PREPARED

The high concern over cyber threats is warranted, as the consequences of failing to address these attacks are severe. Of particular note are reputational loss and existing customer churn, where banks outpace cross-industry averages by 10% and 7%, respectively. Combined, all of these negative consequences are interrelated and ultimately impact business operations and profitable growth. This vulnerability comes at a time when cybercriminals are leveraging AI to outpace traditional defenses, turning fraud into a scalable, lucrative operation.
Percentage of banks reporting these negative outcomes:

FINANCIAL LOSSES

The negative financial consequences since 2022 are staggering. Among the banks surveyed, 60% reported losses between $10M to over $500M during the past two years due to the negative consequences related to cyber threats.



$10M to $99M: Most frequent cost range, affecting a majority of large banks.

$100M to $500M: Common losses among larger banks.

$500M or more: High-cost consequences for the largest banks.

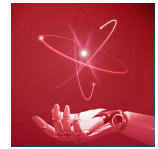
FIGHTING FIRE WITH FIRE

The good news? Banks are starting to recognize that AI isn't just a threat—it's the solution. The intensity of AI adoption varies across sectors, with the banking sector standing out for implementing AI-driven security measures at a rate exceeding the cross-industry average.

This distinction likely reflects the higher stakes within this industry, where the volume of PII data and the consequences of breaches are particularly pronounced. Banks are also more likely than the overall average to say they are leveraging AI to reduce manual tasks and enable faster response times to security incidents.

79% Report leveraging AI to enable faster response time to security incidents

74% Report analyzing cybersecurity data in real-time with AI tools

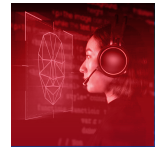


69% Report using AI to analyze historical data and identify vulnerabilities

69% Report automating processes with AI to reduce manual tasks

67% Report using AI to predict future security threats

67% Report deploying AI tools to continuously monitor infrastructure



BENEFITS OF AI-POWERED SOLUTIONS

AI-powered solutions are delivering some tangible results for cybersecurity teams. In the financial services sector, 49% of banks report improved threat intelligence, while 48% say they are better equipped to defend against generative AI-powered attacks. This is especially significant as the financial services sector is often the primary target of cybercriminals who test new attack methods on other industries, like gaming, before deploying them on banks.

The optimism around AI's future impact reflects a growing belief that as AI matures, it will become more adept at addressing the nuances of different types of attacks, from fraud farms to sophisticated AI-driven threats like deepfakes and GPT prompt compromises. Financial services, in particular, are investing heavily in AI to defend against these generative AI-powered attacks, as these industries have the most to lose if their defenses fail.

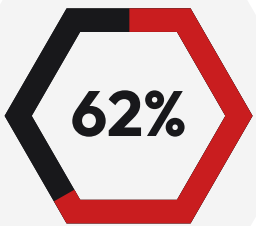
Already Realized Benefits

- Improved threat detection and response
- Improved threat intelligence gathering
- Reduced overall cost of securing my business
- Better defense against basic bot attacks
- Better defense against AI-powered bot attacks
- Better defense against generative AI-powered attacks
- Better defense against human fraud farm attacks

OVERCOMING BARRIERS TO AI ADOPTION

Despite progress, challenges persist. Regulatory restrictions and the global skills gap in AI and cybersecurity expertise remain significant hurdles. Additionally, strict governance policies inhibit rapid adoption. As a result, nearly half of banks struggle to deploy effective AI-powered defenses due to these barriers.

However, banks are finding ways to overcome these obstacles by partnering with specialized vendors. Collaboration with AI-focused cybersecurity providers enables financial institutions to leverage industry-specific solutions, access cutting-edge threat intelligence, and stay compliant with evolving regulations.



Report gaining more value by buying AI-powered cybersecurity solutions than building the solutions in-house

THE STAKES: WHY ACTION CAN'T WAIT

"The AI we're using today is the worst AI there ever will be." That bold assertion from Deutsche Bank Research Analyst Adrian Cox captures the moment: AI capabilities—and our mastery of them—will only advance from here. Yet, as AI improves, so will the sophistication of those who exploit it for fraud.

Meanwhile, the cost of inaction is rising. Banks face mounting pressure from regulators, customers and competitors to strengthen their defenses. And AI continues to evolve, offering criminals new tools to exploit vulnerabilities. For the banking industry, the question is clear: Will you lead the way, or be left behind?

To truly secure their future, banks must invest in AI solutions that not only meet today's challenges but anticipate tomorrow's. This requires a bold approach—embracing innovation, tackling regulatory hurdles, and partnering with experts who can help navigate the complexities of AI-powered security.

The time to act is now. Will your institution rise to the challenge? We invite you to set up a personalized meeting to discuss these results and talk about your needs.

ABOUT ARKOSE LABS

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Trusted by the world's leading consumer brands—including two of the top three banks, Microsoft, Meta, Roblox, and many others—Arkose Labs stops account takeovers, fake account creation, LLM-driven scraping and SMS toll fraud. The platform actively undermines attacker ROI by introducing dynamic friction, making it economically unsustainable for adversaries to persist. Its Security Operations Center (SOC) provides actionable insights from an extensive cross-industry intelligence network, which monitors legitimate traffic and attack patterns across global enterprises. With unparalleled proactive support for internal security teams, Arkose Labs goes beyond conventional security by actively partnering with customers to disrupt organized fraud networks such as Storm-1152. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America."

USA (San Mateo)

Australia (Brisbane)

United Kingdom (London)

Costa Rica (San José)

India (Pune)

Argentina (Buenos Aires)

Book a Meeting