Global ATO Prevention in Banking Market - Focused Insights 2025-2030

Market Report | 2025-05-02 | 111 pages | Arizton Advisory & Intelligence

AVAILABLE LICENSES:

- Single User License $3500.00
- Team License $3650.00
- Enterprisewide $4999.00

Report description:

The global account takeover (ATO) prevention in the banking market is expected to grow at a CAGR of 9.01% from 2024 to 2030.

RECENT VENDOR ACTIVITIES

-On September 12, 2024, Mastercard announced an agreement to acquire global threat intelligence company Recorded Future from Insight Partners for $2.65 billion. This acquisition enhances Mastercard's cybersecurity capabilities, strengthening the insights and intelligence used to protect the digital economy, including the payments ecosystem and beyond.
-On December 4, 2023, Thales announced the successful completion of its acquisition of Imperva. This transaction is expected to create substantial value for Thales' shareholders.

KEY TAKEAWAYS

-By Service Type: The pre-transaction segment accounts for the largest market share of over 48%. Pre-transaction prevention is the security measures used by banks before the transaction to block ATO fraud like MFA, RBA, identity proofing & verification, and device fingerprinting.
-By Development Type: The cloud-based segment is the fastest-growing segment in the market with a CAGR of 10.07%. They have emerged as an important security measure for financial institutions and banks to protect themselves against constantly evolving cyber-attacks.
-By Geography: In 2024, North America accounted for the largest market share, driven by a high incidence of cyberattacks and stringent regulatory requirements.
-Growth Factor: Global account takeover (ATO) prevention in banking market is set to grow due to the growing focus on real-time transaction monitoring and the rise in large-scale phishing attacks.

MARKET TRENDS

Growing Focus Towards Real-Time Transaction Monitoring

With the rise of digital banking, contactless payment, and real-time payment solutions like FedNow in the US, UPI in India, and PIX in Brazil, banks have to keep tracking transactions in real time to avoid ATO attacks. As criminals usually resort to such instant payment networks for transferring money instantly from somewhere, banks need to have real-time fraud engines capable of detecting violating transactions before they even occur. AI-based anti-fraud models scrutinize vast amounts of transaction data in real time to detect anomalies, suspicious patterns, and behavior deviating from normal user patterns. Unlike static rule-based systems, AI is improved by repeated attempts at fraud with each new case, continually improving detection rates. Traditional fraud detection used to depend on post-transaction investigations, where fraudsters had time to cash out the stolen money before banks could act. Real-time monitoring of transactions allows banks to freeze fraudulent transactions during the authorization phase, stopping financial losses and chargebacks. Fraudsters, with open banking and third-party API integrations, take advantage of security loopholes to carry out illicit transactions. Real-time monitoring enables banks to identify suspicious API calls, analyze the level of risk on transactions, and instantly block funds transfers.

Expansion In Biometrics Authentication

Biometric authentication is emerging as a new foundation for ATO prevention in banking, replacing passwords and PINs with fingerprints, facial recognition, voice identification, and behavioral biometrics. It is growing rapidly driven by regulatory requirements, AI capabilities, the growth of digital banking, and customer requirements for frictionless security. Cybercriminals use hijacked credentials from data breaches to conduct ATO fraud. The conventional forms of authentication such as passwords and OTPs over SMS are susceptible to phishing and SIM-swapping attacks. Biometric authentication counters such threats by making it possible for only the legitimate owner to access their account, thereby increasing the market for behavioral biometrics solutions. Contemporary biometric technologies take advantage of AI-driven behavioral biometrics that observe user patterns of behavior such as typing speed, mouse action, and touchscreen activity to identify spoofing behavior. This ensures constant authentication during a user's banking session, making it more difficult for fraudsters to hijack accounts. With users seeking frictionless banking experiences, banks are turning to passwordless biometric authentication. Facial recognition and fingerprint scanning provide a seamless means of logging in without having to remember complicated passwords.

MARKET DRIVERS

Growth In Neobanks & Fintechs

The swift growth of fintech and neobanks is sharply fueling demand for ATO prevention solutions within the banking industry. In contrast to conventional banks, neobanks (online-only banks) and fintech platforms are online-based, hence extremely susceptible to cyber attacks like phishing, credential stuffing, and SIM-swapping attacks. As mobile-first banking solutions have taken the industry by storm, customers want easy and immediate access to their banking products. But greater mobile banking adoption also means more attempts at fraud, which makes ATO prevention the most important task for fintech companies. Chime, a US neobank, used AI-powered fraud detection and device fingerprinting to combat growing ATO efforts. Neobanks and fintech platforms are also pushing their services beyond the confines of traditional banking, connecting with third-party apps via open banking APIs and embedded finance solutions. While this increases customer convenience, it also opens up vulnerabilities, making preventing ATO fraud more important than ever before. Increased usage of digital wallets, peer-to-peer (P2P) transfers, and contactless payments have introduced new fraud threats as hackers try to get unauthorized access to user accounts and associated payment instruments. Neobanks and fintech have to invest in transaction monitoring, fraud detection models, and geolocation tracking to counter threats.

Rise In Large-Scale Phishing Attacks

Increased phishing scams of a sophisticated nature have caused ATO fraud to become a top security threat for banks. In the fourth quarter of 2024, 989,123 cases were reported globally as phishing attacks, by the Anti-Phishing Working Group (APWG) states. Scammers use spoofed email, SMS messages (smishing), and fake customer service phone calls (vishing) to trick customers into revealing login details. Phishing campaigns are becoming more sophisticated due to the spread of AI-powered phishing kits that enable automated fake campaigns. Hackers use machine learning features to create ultra-personalized phishing emails mimicking real bank communication, thus making it difficult for users to detect. Deepfake voice and AI-powered chatbot interventions further increase the success rate of phishing campaigns. As phishing attacks breach passwords, banks are implementing advanced MFA solutions such as biometric authentication, hardware security keys, and mobile app-based authentication to prevent unauthorized access. Governments and regulators are mandating strict cybersecurity standards to restrict ATO fraud caused by phishing. There is a growing demand for robust MFA, AI-driven behavioral analytics, and phishing-resistant authentication as banks seek to shield customers from takeover fraud. Thus, the market has seen a surge in anti-phishing solutions.

SEGMENTATION INSIGHTS

INSIGHTS BY SERVICE TYPE

The global account takeover (ATO) prevention in banking market by service type is segmented into pre-transaction, during-transaction, and post-transaction. In 2024, the pre-transaction prevention segment accounted for the largest market share of over 48%. Pre-transaction prevention is the security measures used by banks before the transaction to block ATO fraud. Different technologies like MFA, RBA, identity proofing & verification, device fingerprinting, and PAM are designed to authenticate genuine users and filter out fake attempts before they result in illegal transactions. ATO attacks have increased in recent years due to data breaches, phishing, and credential stuffing. Cyber attackers use stolen login credentials on the dark web to access financial accounts without authorization. Attackers utilize automated bots to try stolen credentials on various banking platforms. Banks receive millions of fraudulent login attempts every day, which creates a need for AI-powered risk detection. Therefore, banks are implementing MFA, device fingerprinting, and behavioral biometrics to thwart these attacks. AI-driven RBA solutions are going mainstream to block automated and bot-based ATO attacks. Cloud-based fraud detection solutions are becoming popular, enabling real-time monitoring of banking transactions.

INSIGHTS BY DEVELOPMENT TYPE

The global account takeover (ATO) prevention in banking market by development type is categorized into cloud-based and on-premise. The cloud-based segment shows significant growth, with the fastest-growing CAGR of 10.07% during the forecast period. Cloud-based prevention of ATO has emerged as an important security measure for financial institutions and banks to protect themselves against constantly evolving cyber-attacks. With the rise of mobile transactions, open banking APIs, and digital banking, banks need highly scalable, AI-based, and real-time security solutions that cloud-based prevention platforms for ATO offer. The solutions deliver round-the-clock monitoring, AI-powered fraud detection, and unified integration across different banking systems to identify and block account takeovers in real-time. Cloud-based ATO prevention solutions provide scalable infrastructure, artificial intelligence-powered fraud analytics, and real-time threat intelligence to identify suspicious activity and prevent unauthorized access. They allow banks to review millions of transactions in a second and flag suspicious activity instantly. Artificial intelligence (AI) and machine learning (ML) have revolutionized the prevention of ATO by delivering predictive analytics, behavioral biometrics, and real-time anomaly detection. Cloud platforms utilize AI-powered risk scoring, fraud pattern analysis, and identity proofing to block fraudulent transactions from happening in the first place.

GEOGRAPHICAL ANALYSIS

In 2024, North America accounted for the largest share of the global ATO prevention in banking market. An increase in advanced

cybercrime techniques is one of the primary growth drivers for the ATO prevention market. Cyber attackers are leveraging deepfake AI-powered technology, credential stuffing attacks, phishing attacks, and social engineering tactics to bypass traditional security mechanisms. Increased instances of authorized push payment scams and synthetic identity theft have fueled the demand for efficient ATO prevention. As threats become dynamic, banks are subjected to pressure to adapt new-age security strategies to prevent ATO. Another main driver in the ATO prevention market in North America is the rapid expansion of digital banking offerings and mobile payment systems. Consumers prefer increasingly mobile banking apps, contactless payments, and peer-to-peer payment services like Zelle, Venmo, and Cash App. While these technologies provide increased convenience, they also open new attack vectors for criminals. With more consumers going digital, so does the demand for more aggressive security controls.
The APAC region shows the highest growth of global ATO prevention in banking market during the forecast period. The region is experiencing rapid digitalization, leading to a surge in online banking services. This growth has attracted cybercriminals, resulting in a heightened focus on ATO prevention. Banks are adopting technologies like biometric authentication and AI-driven fraud detection. The market is in a rapid growth phase, fueled by expanding consumer bases and increasing investments in infrastructure.

COMPETITIVE LANDSCAPE

The global account takeover (ATO) prevention in banking market report consists of exclusive data on 24 vendors. The market is highly competitive, with vendors trying to distinguish themselves through technology innovation, comprehensive offerings, and partnerships. The competitive environment is influenced by technology innovation, regulatory compliance, and customer experience. New entrants in the market have difficulty differentiating themselves because of the intense brand presence of well-established cybersecurity companies. Well-established banks like to have long-term relationships with highly reputable suppliers, thus making it difficult for new entrants. The market is vulnerable to low-cost, low-quality security solutions that provide only minimum fraud detection. These inferior products introduce security vulnerabilities. The future of ATO prevention will be informed by innovative technologies that are security-focused, friction-reducing and accuracy-improving fraud detection. Vendors will further break away from the use of passwords and OTPs and move toward the adoption of behavioral biometrics, AI-ML technology, and frictionless authentications.

Key Vendors
- Datavisor
- Entrust
- Experian
- Kount
- LexisNexis Risk Solutions
- Ping Identity

Other Prominent Vendors
- Accertify
- Arkose Labs
- BioCatch
- Bureau
- Combate a Fraude (Caf)
- Callsign
- Entersekt
- Feedzai
- Human
- Imperva

-Mastercard
-Outseer
-Prove Identity
-Socure
-SpyCloud
-Telesign
-Transmit Security
-TransUnion

SEGMENTATION & FORECASTS

-By Service Type
oPre-Transaction
oDuring-Transaction
oPost-Transaction
-By Deployment Type
oCloud-Based
oOn-Premise
-By Geography
-North America
oUS
oCanada
-Europe
oUK
oGermany
oFrance
oItaly
-APAC
oChina
oIndia
oAustralia
oJapan
-Latin America
oBrazil
oMexico
-Middle East & Africa
oTurkey
oSaudi Arabia

KEY QUESTIONS ANSWERED:

1.What is the expected growth of the global ATO prevention in banking market?
2.What is the growth rate of the global ATO prevention in banking market?
3.What are the factors driving global ATO prevention in banking market growth?
4.Which region will have the highest CAGR in the global ATO prevention in banking market?
5.Who are the major players in the global ATO prevention in banking market?

Table of Contents:

CHAPTER - 1: Global ATO Prevention in Banking Market Overview
-Executive Summary
-Key Findings
-Key Developments

CHAPTER - 2: Global ATO Prevention in Banking Market Segmentation Data
-Service Type Market Insights (2021-2030)
oPre-Transaction
oDuring-Transaction
oPost-Transaction
-Deployment Type Market Insights (2021-2030)
oCloud-Based
oOn-Premise

CHAPTER - 3: Global ATO Prevention in Banking Market Prospects & Opportunities
-Global ATO Prevention in Banking Market Drivers
-Global ATO Prevention in Banking Market Trends
-Global ATO Prevention in Banking Market Constraints

CHAPTER - 4: Global ATO Prevention in Banking Market Overview
-Global ATO Prevention in Banking Market -Competitive Landscape
-Global ATO Prevention in Banking Market - Key Players
-Global ATO Prevention in Banking Market- Key Company Profiles

CHAPTER - 5: Appendix
-Research Methodology
-Abbreviations
-Arizton

SCOTTS INTERNATIONAL

Global ATO Prevention in Banking Market - Focused Insights 2025-2030

Market Report | 2025-05-02 | 111 pages | Arizton Advisory & Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$3500.00
	Team License	$3650.00
	Enterprisewide	$4999.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-17
		Signature	