Liminal™ | link™ by Liminal

Link Index

Account Takeover Prevention in Banking

July 2024 | Strictly Confidential

Contents

Navigation – click the Liminal logo to return to this page.

Executive Summary: Market Overview

Key Takeaways

- **ATO prevention defends against a wide range of threats.**
  Account takeover (ATO) is a type of third-party fraud where a malicious actor gains unauthorized access to a user's account, enabling them to steal funds, sensitive data, or initiate fraudulent transactions. Unauthorized access is typically achieved through phishing or by exploiting user credentials obtained via data breaches or malware. ATO threats come in various forms, including credential stuffing, phishing, social engineering, malware, SIM swapping, and man-in-the-middle attacks.

- **ATO can lead to severe financial consequences, especially for banks.**
  The consequences of ATO can be severe, often resulting in significant financial losses for the user or the institution where the account is maintained. Average losses can range from about $6,000 to $13,000 USD per ATO incident in the banking industry.[1] The full scope of the ATO costs banks incur remains difficult to quantify, as banks are reluctant to publicly divulge the frequency and value of successful ATO attacks.

- **Fraudsters are becoming more effective, and vendors are counteracting with sophisticated solutions.**
  As ATO prevention methods have become more effective at thwarting simplistic attacks like credential stuffing, fraudsters have shifted their focus to deceiving individuals through phishing and social engineering tactics. Specifically, banks have seen a sharp rise of 66.8% in social engineering attacks over the last two years.[1] In response, solution providers have developed sophisticated detection methods utilizing multi-factor authentication, biometrics, and passive behavioral signals to identify anomalous behavior. Banks are adopting these advanced techniques to reduce fraud losses, as their user accounts hold significant value.

Current Challenges

- **Large-scale phishing attacks.** Phishing is the most common ATO attack, responsible for 26.7% of all ATO incidents among the eight primary attack methods.[1]
- **Account recovery vulnerability due to login defense prioritization.** 94% of banks recognize account recovery as a threat yet are more likely to prioritize login defense.[1]
- **Inadequate protection of mobile channels.** Banks report that most ATO attacks originate from mobile apps, yet only 44% utilize mobile device signals for protection.[1]

Future Demands

- **Social engineering and scam detection.** 84% of bank ATO solution seekers highly demand social engineering and scam detection, the second most buyer-requested capability.[1]
- **Behavioral signals.** Banks increasingly demand passive capabilities like behavioral biometrics, with 81.8% of those not currently using them planning to adopt them within the next two years.[1]
- **Passwordless authentication.** Over 40% of consumers consider traditional password-based authentication insecure, adding pressure for banks to transition towards passwordless solutions.[2]

Key Purchasing Criteria (KPC)

- **Accuracy:** 90% of ATO solution buyers at banks prioritize accuracy.[1]
- **User Experience:** 86% of ATO solution buyers at banks prioritize user experience.[1]
- **Product Integration:** 84 of ATO solution buyers at banks prioritize product integration.[1]
- **Customization:** 82% of ATO solution buyers at banks prioritize customization[1]

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)
(2) ATO Prevention Consumer Survey, April 2024 (N=511)

Executive Summary: Vendor Landscape

Liminal's ATO Prevention in Banking landscape analysis identifies the top vendors that address the fraud threats facing financial institutions today. With criminal actors deploying a wide range of attack vectors that include phishing, social engineering, and credential stuffing, a fragmented solutions landscape has emerged with vendors taking specialized approaches to address ATO attacks that can be grouped into three primary categories: Authentication-focused vendors, Fraud-focused vendors, and Identity-focused vendors. Fraud-focused vendors use probabilistic data, including behavioral signals, to protect against fraud, mainly at the transaction level, while authentication-focused vendors use comprehensive authentication capabilities to prevent unauthorized access during login. Identity-focused vendors combine select capabilities of both authentication and fraud prevention methods, using identity as the bedrock.

The analysis highlights 24 leading companies, selected based on an evaluation of their product offerings, strategies, and market presence.

Landscape Analysis

- **The market is split into fraud, authentication, and identity vendors.** Solution providers in the ATO landscape employ diverse strategies, with some exhibiting limited capability overlap.
- **Banks leverage multiple vendors in their tech stack.** Vendors with unique capabilities collaborate to offer comprehensive coverage.
- **Credit bureaus and card issuers hold strong market presence.** Experian, TransUnion and Mastercard are all ranked within the top 5 for market presence.
- **Overall satisfaction is most strongly correlated with scalability.** Despite being ranked fifth among KPCs, buyer satisfaction showed the highest correlation with satisfaction in scalability.

Key Benefits of Leading Account Takeover Solutions

- **Reduction in successful ATO attacks:** Highly accurate solutions limit the amount of ATO attacks that lead to financial loss by 64%.[1]
- **Reduction in average fraud loss:** Leading solutions effectively minimize average fraud losses, reducing them by 52%.[1]
- **Reduction in customer abandonment:** By providing a seamless user experience, leading solutions reduce customer abandonment by 24%.[1]

Top 24 Vendors for Account Takeover Prevention in Banking

Accertify, Arkose Labs, BioCatch, Bureau, caf., callsign, DATAVISOR, entersekt, ENTRUST, experian., feedzai, HUMAN, Kount, LexisNexis RISK SOLUTIONS, mastercard, neuroID, OUTSEER, PingIdentity, Prove, Socure, SpyCloud, telesign, transmit security, TransUnion

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

The adoption of passwordless authentication and the widespread availability of generative AI are fundamentally reshaping the ATO threat landscape.

Digital banking fraud is big business in 2024, with the bulk of ATO attacks perpetrated not by sole actors but by well-coordinated and financed criminal groups working at scale from jurisdictions across the globe. In this increasingly institutionalized attack environment, bank accounts have emerged as prized ATO targets due to the high profitability of a successful attack.

This ATO threat landscape is being shaped by two wider trends: continued adoption of more secure passwordless authentication technologies by banks, and the widespread availability of powerful generative AI tools to fraudsters. Passwordless authentication is raising the cost and technical capabilities required for illicit actors to compromise an account via phishing and other forms of credential theft. Technologies like FIDO2 Passkeys make phishing effectively impossible. In parallel, generative AI is making the deployment of current fraud techniques more scalable, cost effective, and executable by criminals who lack requisite technical or language skills.

These trends account for the continued rise of social engineering or "scam" attacks as an overall percentage of successful ATO attempts as fraudsters adapt to the increasing challenge of defeating the more rigorous authentication methods adopted by financial institutions. The current vendor landscape for ATO Prevention reflects this shifting risk environment, with platforms taking one of several general approaches toward addressing increasingly sophisticated threats.

Authentication-focused vendors seek to address threat vectors that fundamentally compromise a user's login credentials via phishing or data breaches. This approach can be likened to upgrading the physical security of a home's front door to make it resistant to lock picking or the physical breach.

In contrast, fraud-focused vendors seek to quantify the risk of a user's session and the resulting transactions after the session has already been authenticated. Or, in home security terms, deploying security cameras inside a house to observe when criminals are walking around inside and notify the police. As each of these approaches are suited to detect specific types of attacks, banks today typically deploy multiple vendors within their tech stack to build layered defenses.

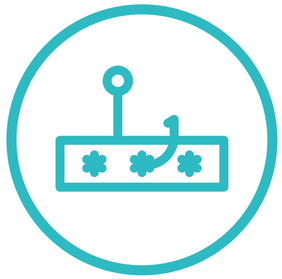
The newest entrants into the ATO prevention space, identity-focused vendors take an approach that follows the evolution of IT Security defenses used to protect banks and other institutions against cybersecurity threats at the fundamental platform level. They transition away from solutions that focus on securing the network perimeter or endpoint devices themselves and instead take an identity-centric approach. Current identity-focused ATO vendors combine features from authentication- and fraud-focused approaches, built on top of a clear understanding of the underlying identity of the accountholder themselves.

Liminal™ | link™ by Liminal

LINK INDEX

Market Overview

The continued prevalence of phishing attacks, diminished prioritization of account recovery, and mobile ATO attacks pose challenges for banks



Phishing continues to be the most significant ATO threat vector

Among the eight primary attack methods, phishing accounts for 26.7% of all account takeovers, making it the most common threat.[1]

Banks face significant challenges in protecting their customers from phishing attacks, particularly as fraudsters embrace new technologies like generative AI.

Account recovery continues to be a weak point as banks prioritize login defense

Over three times as many banking respondents view login as a major concern; however, 94.0% acknowledge that account recovery is also a significant threat.[1]

Weak account recovery protocols can significantly increase account takeovers and financial losses.

Banks are failing to adequately protect mobile channels

Banks report that the majority of ATO attacks originate from mobile apps rather than mobile web or desktop, yet only 44.0% utilize mobile device signals for protection.[1]

Neglecting mobile device signals presents a significant risk to the banking industry, particularly as mobile channels continue to grow in prevalence.

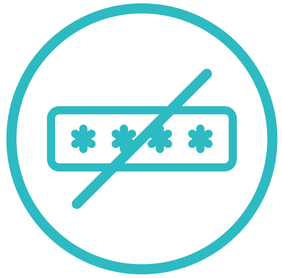
(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Banks look for highly accurate ATO prevention solutions from third party-vendors that leverage biometric signals and address scam attack threats

Challenge	Causes	Customer Demands
Banks with limited ATO protection experience more than 45,000 successful fraud attacks a year.[1]	Ineffective solutions fail to accurately detect fraudsters, permitting unauthorized access to sensitive accounts.	Accuracy is the most demanded key performance criterion, with over 90% of banking respondents prioritizing it.[1]
Consumers are dissatisfied with traditional usernames and passwords, with only 59.9% of consumers considering them secure for their bank accounts.[2]	Consumers must manage numerous username and password combinations that are challenging to remember and vulnerable to ATO.	Eighty-eight percent of banking decision-makers prioritize biometric authentication, largely due to the widespread use of FaceID and TouchID.[1]
Banks find it challenging to deliver the frictionless experiences consumers enjoy in other industries, like eCommerce and social media.	Many ATO vendors employ active authentication prompts, such as SMS OTPs and magic links, which disrupt the user experience.	Banks are demanding passive capabilities like behavioral biometrics, with 81.8% of those not currently using them planning to adopt them within two years.[1]
Banks have experienced a 66.8% increase in social engineering attacks over the past two years.[1]	Generative AI tools are enhancing social engineering by making attacks more believable and scalable.	Eighty-four percent of banking decision-makers highly value social engineering and scam detection, making it the second most sought-after capability.[1]
Banks struggle to implement sophisticated ATO prevention in-house.	High maintenance costs and a lack of internal engineering expertise hinder banks' ATO prevention efforts.	Eighty percent of banks have not considered bringing solutions in-house, and only 10% plan to do so in the next two years, illustrating a preference for vendor solutions.[1]

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)
(2) ATO Prevention Consumer Survey, April 2024 (N=511)

Customers want solutions that can provide frictionless experiences, behavioral signals, passwordless authentication, and regional customization



	Frictionless Experience	Behavioral Signals	Passwordless Authentication	Regional Customization
Description	Ensuring robust account security while minimizing user friction.	Using the patterns and characteristics of user behavior, such as typing speed and mouse movements, to prevent ATO attempts.	Authenticating a user without the use of traditional passwords, instead relying on biometrics, security keys, or other methods.	Deploying ATO solutions that remain compliant with evolving national and state-level privacy and data protection regulations.
Blockers	Friction-Filled Authentication Methods Security Concerns	High Cost Extensive Implementation Process	Password Stickiness Legacy System Integrations	Fragmented Privacy Landscape Regional Vendor Focus

AI/ML tools, FIDO2 standards, and the ubiquity of biometric authentication from Big Tech aid banks in the fight against account takeover fraud

Vendors provide sophisticated AI / ML fraud detection methods

Solution providers are increasingly leveraging sophisticated machine learning and artificial intelligence to detect advanced fraud techniques, such as social engineering and man-in-the-middle attacks. These tools analyze a wide range of signals to identify anomalies, preventing fraudulent actors from stealing funds.

FIDO2 paves the way for more secure authentication

FIDO2 authentication is an open standard that uses public key cryptography to enable secure, passwordless logins across devices and platforms.[1] It is important in protecting against account takeovers because it eliminates the risks associated with traditional passwords, such as phishing and credential theft, by relying on strong cryptographic keys stored on users' devices.

Big Tech has made biometric authentication ubiquitous

Device manufacturers like Apple have seamlessly integrated biometric authentication into consumers' everyday lives with products like FaceID and TouchID. Device-native biometric authenticators can be easily integrated into banks' onboarding and login processes, enhancing user experience without compromising security.

(1) FIDO Alliance

Vendors struggle to address social engineering, lack a strategy for handling Big Tech data restrictions, and struggle to cover the complete customer lifecycle

Only a portion of vendors can address the growing social engineering threat

Eighty-four percent of banks highly demand social engineering and scam detection, making it the second highest demanded product capability. However, only about 3 in 5 of the top vendors offer this capability. Many banks may continue to struggle with social engineering, which has resulted in a reported increase of 66.8% in financial losses over the past two years.[1]

Solution providers are unsure how to deal with Big Tech data restrictions

Ninety-six percent of banking professionals believe restricting access to device signals could compromise their ATO solutions - additionally, 90% share similar concerns over losing other data signals, such as third-party cookies. ATO prevention solutions may face significant challenges from Big Tech data restrictions, particularly when attempting to fingerprint devices.[1]

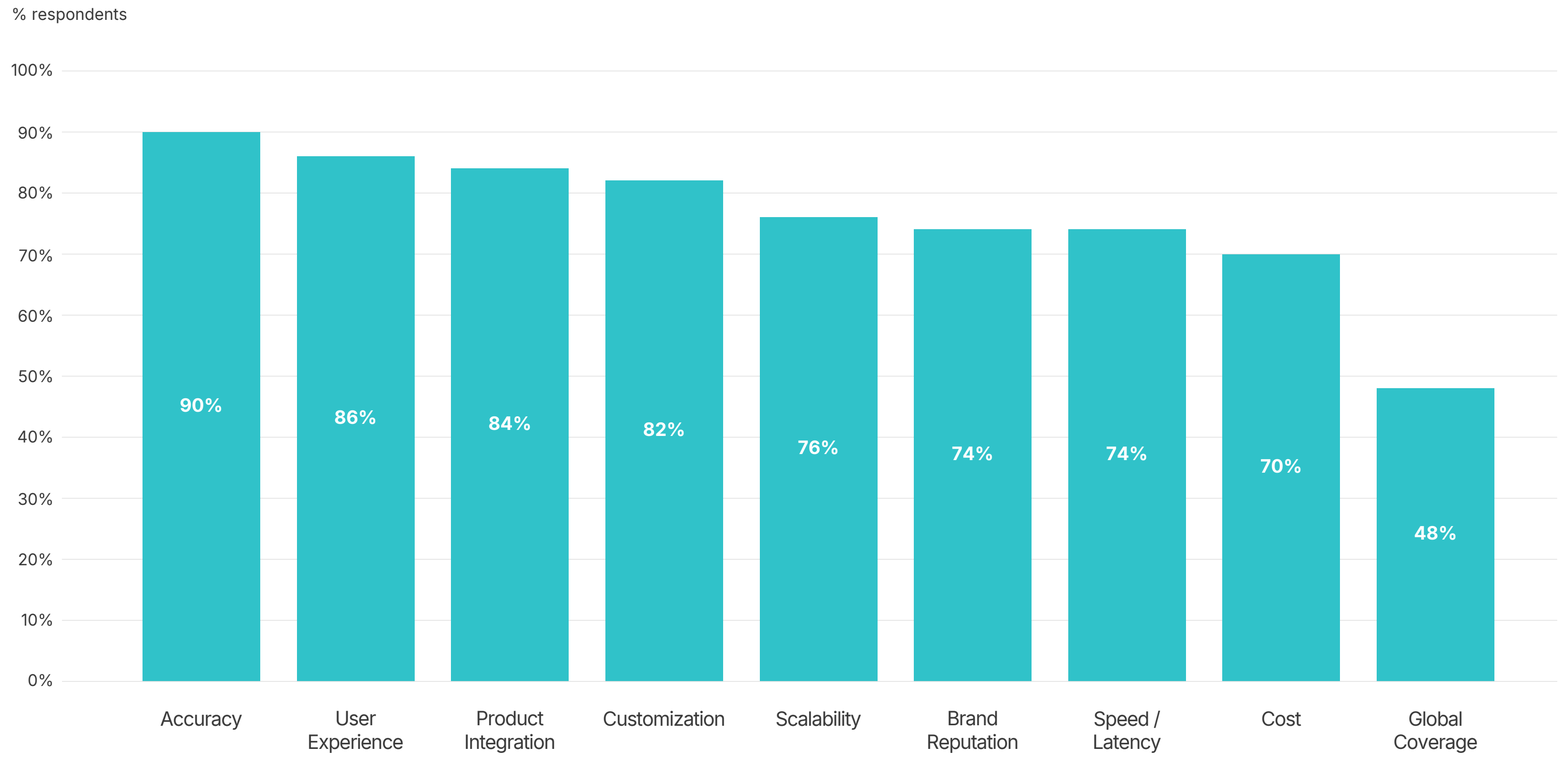
Few vendors offer unified platform solutions

The ATO prevention market is fragmented into fraud, authentication, and identity vendors. While many banks utilize multiple vendors in their tech stack, few vendors offer platform solutions that cover the entire user lifecycle.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Banks most highly prioritize accuracy, user experience, product integration, and customization when purchasing ATO prevention solutions

Key Purchasing Criteria for ATO Prevention Solutions in Banking[1]



(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Top vendors can achieve significant reductions in successful ATO attacks, average fraud losses, and customer abandonment

Reduction in Successful ATO Attacks[1]

Banks employing leading vendors experience an average of around 16,000 successful ATO incidents annually, nearly three times fewer than banks using lagging solutions.[1]

Reduction in Average Fraud Loss[1]

Leading solution providers reduce the average fraud losses by more than half, from $13,400 to $6,430 USD.[1]

Reduction in Customer Abandonment[1]

By limiting friction during onboarding, login, transaction, and account recovery processes, customers of leading ATO vendors may experience a decrease in abandonment rates from 19.8% to 15.1%.[1]

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Banks can reduce fraud losses by nearly $500 million while also seeing significant operational cost and customer retention savings[1]

Reduction in Fraud Losses[2]	**Lagging Solution**	**134,000** Successful fraud incidents	×	**34%** Share of losses related to ATO	×	**$13,430** Average ATO loss	÷	**37 M** Average customer base	=	**~$16 fraud loss per customer**	**~$12 in fraud loss savings per customer**
	Leading Solution	**77,000** Successful fraud incidents	×	**21%** Share of losses related to ATO	×	**$6,400** Average ATO loss	÷	**26 M** Average customer base	=	**~$4 fraud loss per customer**	
Operational Cost Savings[2]	**Lagging Solution**	**3** Employees required to handle ATO incident	×	**$21** Employee hourly wage	×	**6.1** Average hours spent per employee			=	**~$390 total cost**	**~$26 in savings per ATO incident**
	Leading Solution	**3** Employees required to handle ATO incident	×	**21%** Employee hourly wage	×	**5.7** Average hours spent per employee			=	**~$364 total cost**	
Customer Retention Savings[2,3]	**Lagging Solution**	**15%** Customer retention rate	×	**$4,500** Average customer LTV					=	**~$675 customer value captured**	**~$215 in customer retention savings**
	Leading Solution	**20%** Customer retention rate	×	**$4,500** Average customer LTV					=	**~$900 customer value captured**	

(1) The average bank size of respondents was about 28 M customers. Further calculations and sources can be found in the appendix.
(2) ROI data captured from Liminal Market Demand Survey, March 2024, N=50.
(3) Customer retention rates can be influenced from several factors, and may not be fully attributed to ATO solutions.

Link Index

Banks consider biometric authentication, continuous authentication, and social engineering and scam detection key capabilities for ATO prevention

Demand[1]	Product Capabilities
H	App-based Authentication
H	Biometric Authentication
H	Continuous Authentication
H	Data Breach Monitoring
H	Email-based One-Time Passcode
M	SMS / Phone One-Time Passcode (SMS OTP)
M	Social Engineering and Scam Detection
M	Behavioral Biometrics
M	Device Risk Scoring
M	Location Intelligence
M	Proxy And VPN Detection
M	SIM Swap Detection
M	Time-based One-Time Passcode (TOTP)
M	Behavior Analytics
L	Bot Detection
L	FIDO2 Authentication
L	Knowledge-Based Authentication
L	Magic Links
L	Signal Sharing Network
L	User Risk Scoring

H High Demand M Medium Demand L Low Demand

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Other Factors For Consideration

Accuracy

Accurate solutions effectively decrease the amount of fraud losses without false positives, ensuring a secure and safe solution.

Buyer Satisfaction

Solution providers with robust customer support and responsiveness to customer needs deliver high satisfaction for banks.

Customization

Customizable solitons allow for the adjusting risk-scoring models, configuring rules, and setting up alerts/notifications.

Product Integration

Solutions with strong product integration require minimal time and resources to implement ATO prevention measures effectively.

Scalability

Scalable solutions maintain their effectiveness, regardless of the volume of logins, transactions, and account recovery attempts.

Future buyers will demand cost-effective behavioral signals and passwordless authentication solutions with strong user experience (UX)

Behavioral Capabilities

- Behavioral Analytics
- Behavioral Biometrics
- Bot Detection

Passwordless Capabilities

- Device-based / Cloud-based Passkeys
- QR Code Authentication
- WebAuthn

Additional Factors for Consideration

Cost

Customer perception of the cost-effectiveness of their ATO prevention solution can be influenced by pricing models, supplemental services, and additional capabilities that surpass those of competitors.

User Experience

Vendors offering strong UX provide strong fraud detection alongside minimal friction, limiting customer abandonment rates.

(1) See Appendix for Definitions of Product Capabilities

Brand awareness, leadership, market penetration, company size, and employee growth are the key market presence criteria for ATO prevention vendors

Brand Awareness

A well-known vendor will be able to capture more customers. We gauged the awareness of each vendor for their ATO prevention solution among buyers in banking.

Company Size

Large vendors possess the stability and the capacity to accommodate bigger clients, thus driving larger revenues. We compiled employee headcount data and compared top companies.

Employee Growth

Vendors experiencing headcount growth indicate strong prospects for revenue growth and position it as a more formidable player in the market. We calculated year-over-year growth and compared vendors to each other.

Market Leadership Perception

Vendors perceived as market-leading are better positioned to capture market share. We surveyed ATO prevention customers in banking to analyze the levels of customer satisfaction across vendors.

Market Penetration

Having more customers increases your presence in the market. We surveyed banks to analyze the most frequently used vendors.

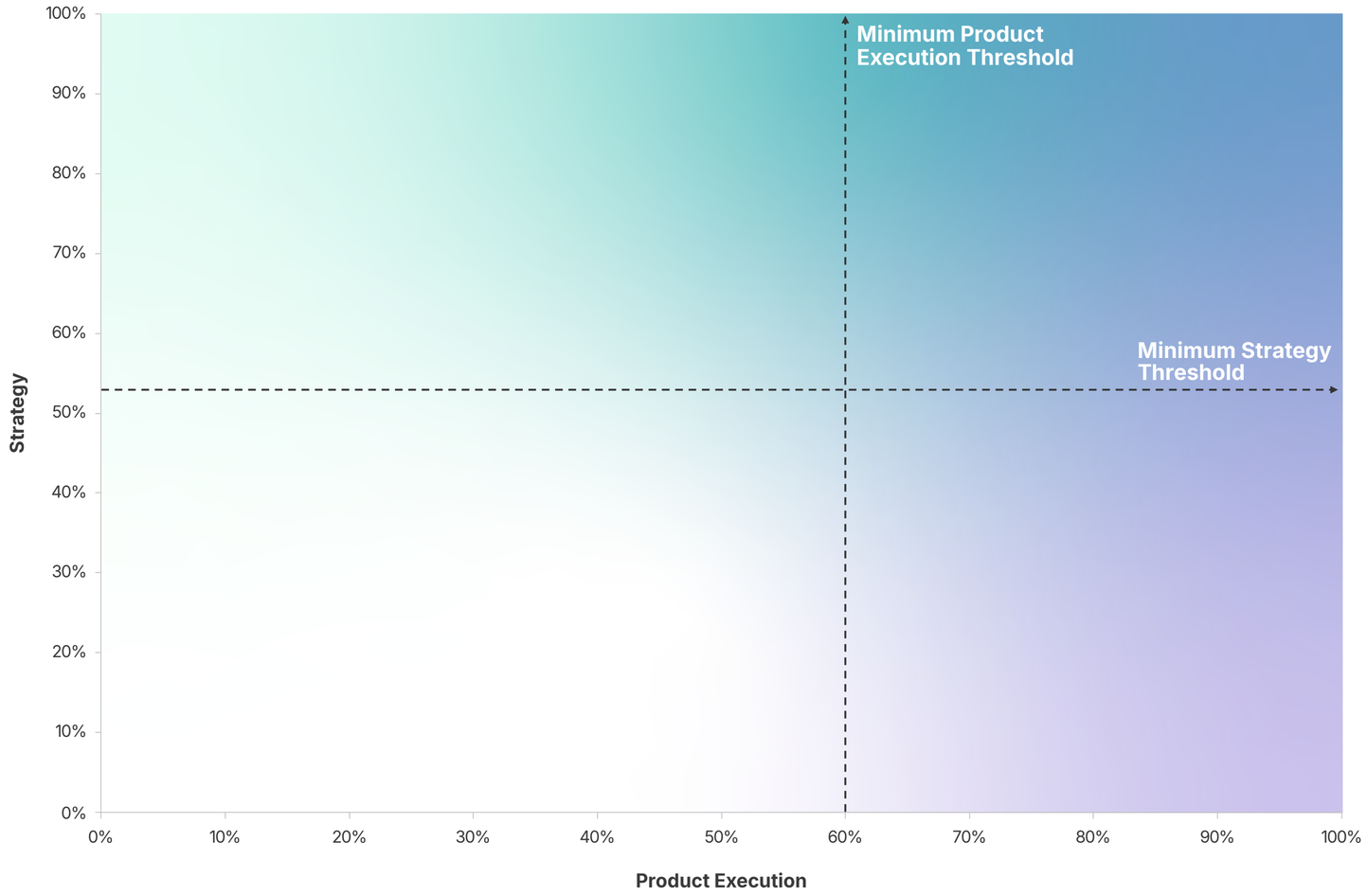
To identify the leading vendors in ATO Prevention in Banking, we set benchmarks for minimum product execution and strategy

Minimum Product Execution Threshold

To establish a minimum product execution threshold, we surveyed financial services buyers to identify the most highly valued capabilities for ATO prevention capabilities. By prioritizing capabilities according to demand, we determined that a company needs a minimum product execution score of 60% to sufficiently meet product capability demand.

Minimum Strategy Threshold

We established a leadership strategy threshold by analyzing critical future demand elements, behavioral signals, and passwordless authentication capabilities. Leading vendors attain a minimum strategy score of 53%.



Of the 56 companies analyzed, 27 met minimum product execution requirements, with 24 classified as Leading Vendors

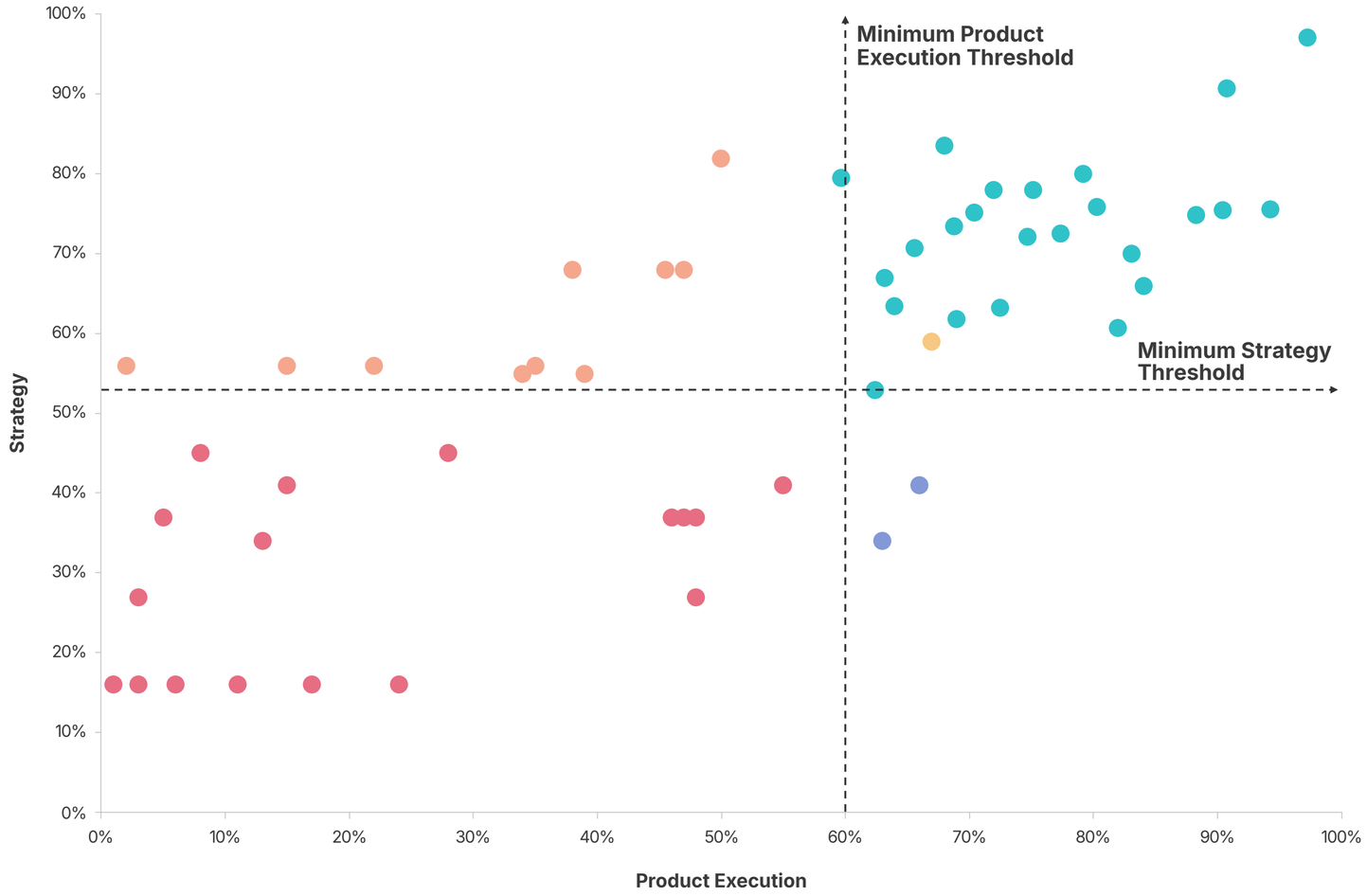
Leading Vendors
Strong overall solutions that possess the must have product and strategic capabilities for this use case

Product-Focused Vendors
Solutions with strong product capabilities but do not meet the strategy score threshold

Adjacent Vendors
Strong overall solutions but do not have the required capabilities for this market use case

Specialized Vendors
Solutions that can solve for a part of the use case but do not have all must have capabilities

Adjacent Leaders
Solutions with capabilities that compete with leading vendors but are not primarily focused on serving this use case



Vendor positioning on the Link Index for ATO Prevention in Banking

LEADING VENDORS

- Accertify
- Arkose Labs
- BioCatch
- Bureau
- Caf
- Callsign
- DataVisor
- Entersekt
- Entrust
- Experian
- Feedzai
- HUMAN
- Kount
- LexisNexis Risk Solutions
- Mastercard
- NeuroID
- Outseer

LEADING VENDORS

- Ping Identity
- Prove
- Socure
- SpyCloud
- Telesign
- Transmit Security
- TransUnion

PRODUCT-FOCUSED VENDORS

- Nevis Security
- Uniken

ADJACENT VENDORS

- Deep Labs
- Fortinet
- Imperva
- Instnt
- Nethone
- OneSpan
- Seon

SPECIALIZED VENDORS

- Akamai Technologies

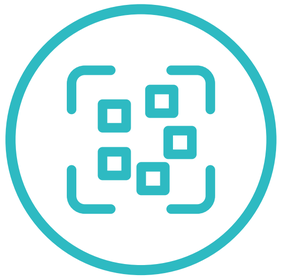
SPECIALIZED VENDORS

- Alessa
- Anonybit
- Duo Security
- GBG
- GeoComply
- IBM
- Incognia
- iProov
- Keyless
- Palo Alto Networks
- SecureAuth
- SHIELD
- Stytch
- TMT ID
- Veridium
- ZeroFox

ADJACENT LEADERS

- 1Kosmos

Leading vendors have three distinct focuses: authentication, fraud prevention, and identity



Vendors have distinct focuses when combatting ATO

Most vendors focus on authentication, fraud prevention, or identity approaches.

Solution providers in the ATO landscape have differentiated strategies and some have limited capability overlap.

Banks leverage multiple vendors in their tech stack

Vendors with differentiated capabilities work alongside each other to provide comprehensive coverage.

Fraud, authentication, and identity capabilities complement each other to cover the entire customer lifecycle.

Credit bureaus and card issuers have strong market presence

Experian, TransUnion, and Mastercard all rank within the top 5 for market presence.

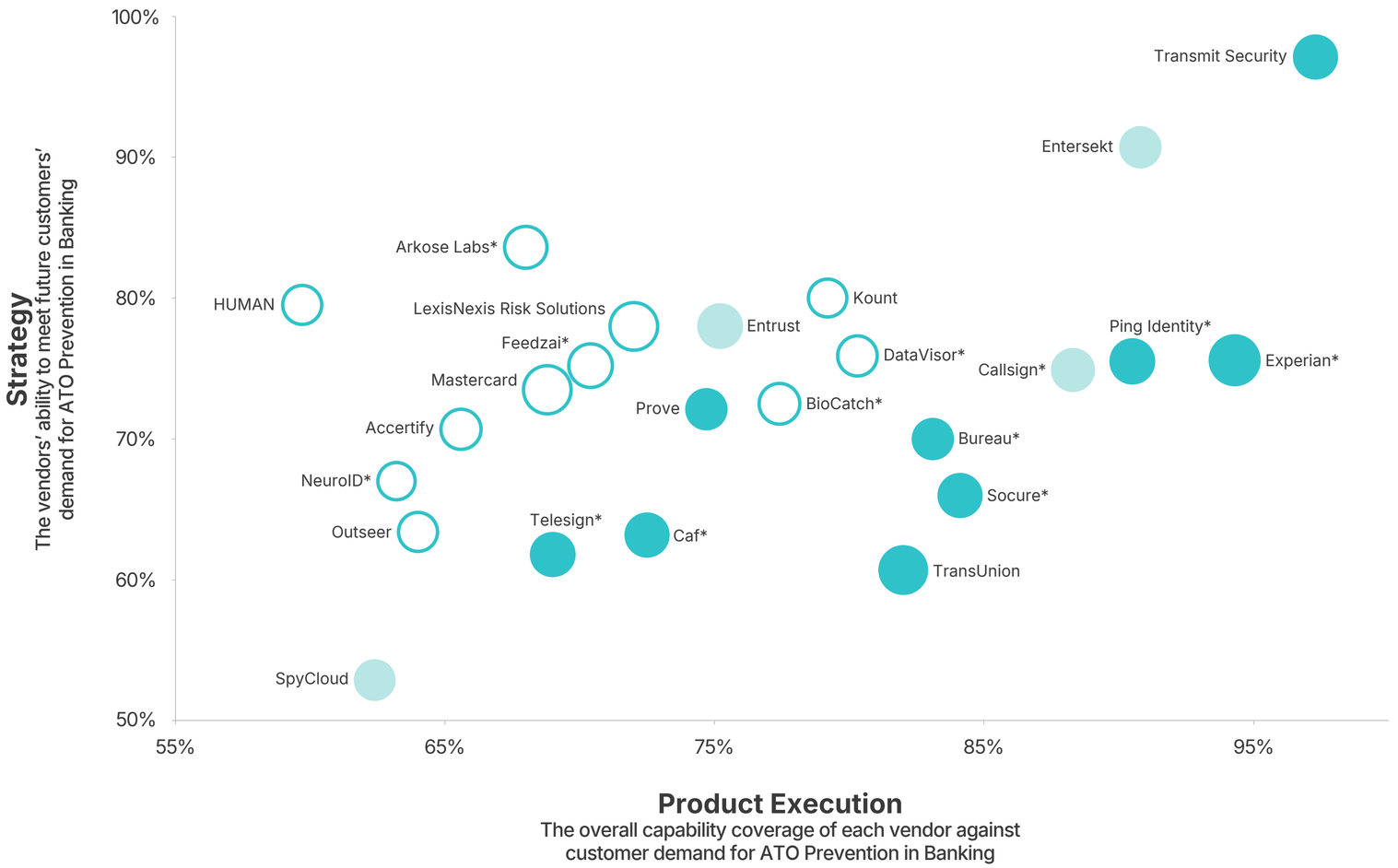
These companies can leverage their extensive data assets to fine-tune models and accurately detect ATO.

Overall satisfaction has highest correlation with scalability

Despite being the 5 ranked KPC, buyer satisfaction saw the highest correlation with scalability satisfaction.

Scalability is vital for banks to handle increasing volumes and evolving fraud tactics efficiently.

Link Index for Account Takeover Prevention in Banking: Leading Vendors



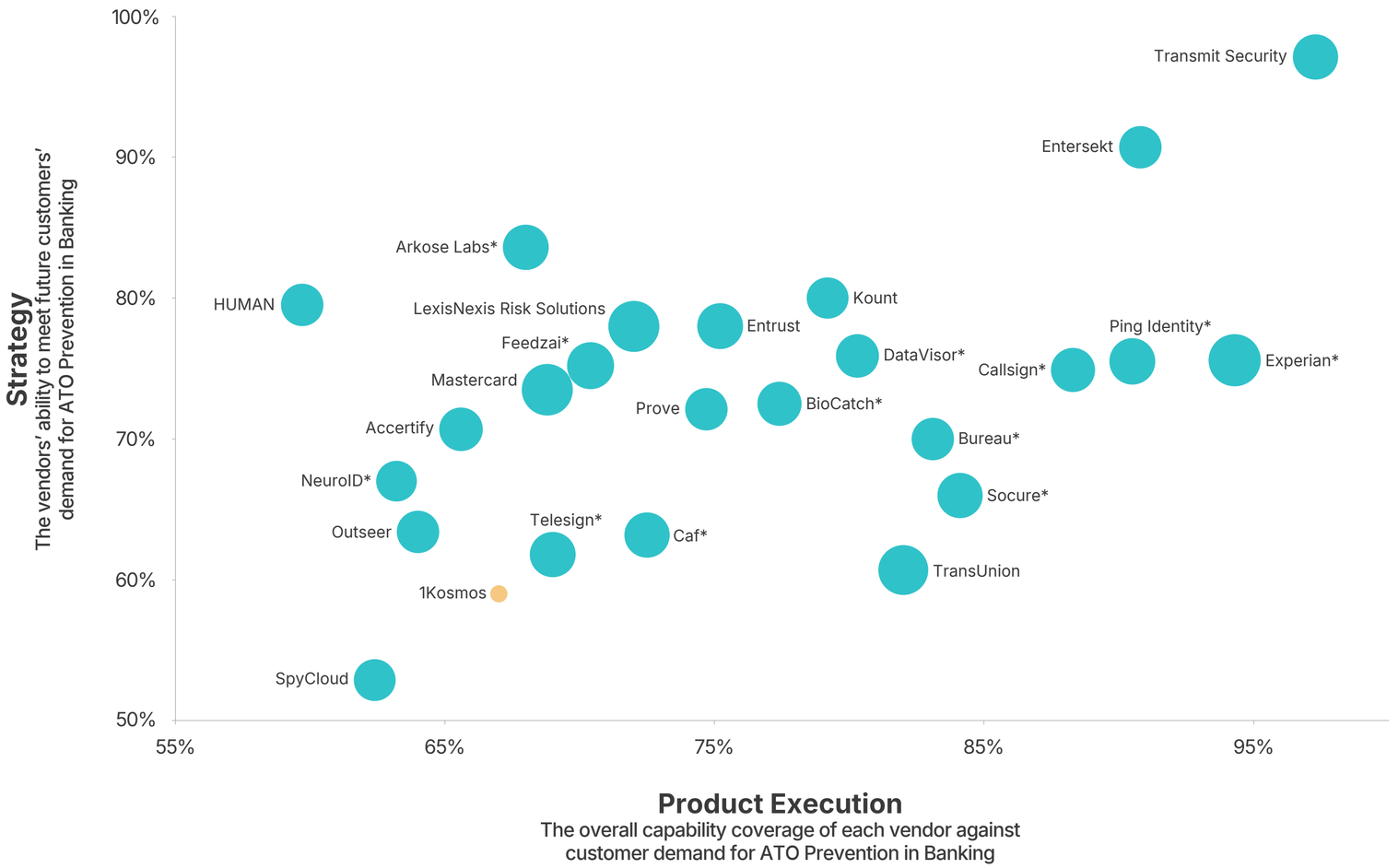
Fraud-Focused Vendors
These solutions use probabilistic data, including behavioral signals, to protect against fraud mainly at the transaction level

Authentication-Focused Vendors
These solutions use comprehensive authentication capabilities to prevent unauthorized access to accounts during login

Identity-Focused Vendors
These solutions take a hybrid approach, combining authentication and fraud prevention methods, with identity acting as the bridge between the two

Note: Companies with an asterisk (*) participated in an Analyst Briefing with Liminal for this report. Bubble Size on the Link Index displays size of Market Presence.

Link Index for Account Takeover Prevention in Banking: Leading Vendors and Adjacent Leaders



Leading Vendors

Strong overall solutions that possess the must have product and strategic capabilities for this use case

Adjacent Leaders

Solutions with capabilities that compete with leading vendors but are not primarily focused on serving this use case

Note: Companies with an asterisk (*) participated in an Analyst Briefing with Liminal for this report. Bubble Size on the Link Index displays size of Market Presence.

Liminal™ | link™ by Liminal

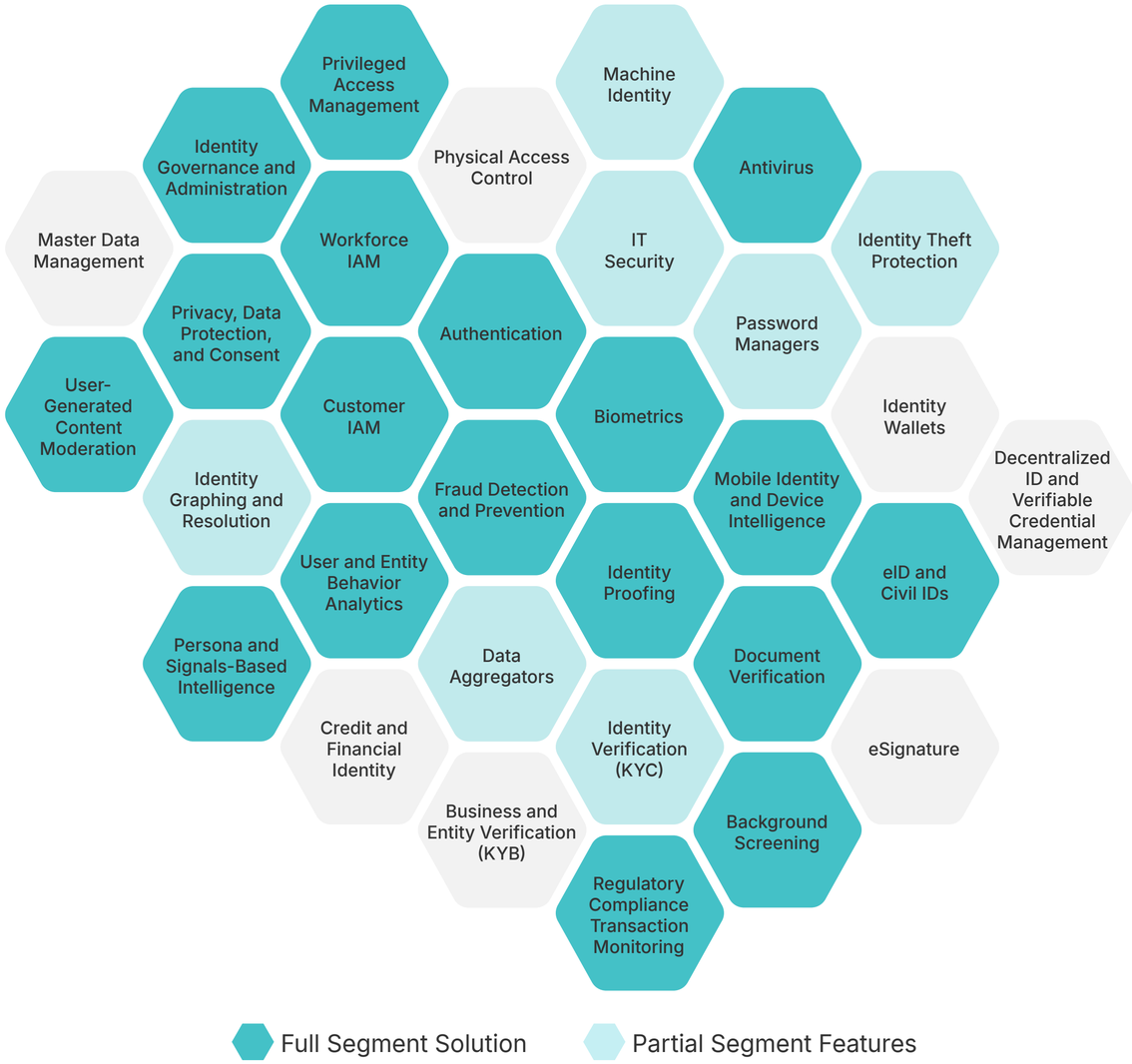
LINK INDEX

Vendor Overview

Entersekt

Entersekt provides secure authentication and payment solutions, focusing on protecting digital transactions. It offers multi-factor authentication, biometric authentication, and mobile app security to safeguard user identities and financial activities. The platform integrates with existing systems to provide seamless, real-time security across various channels, including online banking, mobile apps, and E-commerce.

Company Information[1]	
Headquarters	Atlanta, Georgia
No. of Employees	358 as of May 2024
Last Raised	Venture – Series Unknown in June 2022 (Amount Undisclosed)
Primary Segment	Authentication, Fraud Detection and Prevention
Vertical Focus	Financial Services
Geographic Focus	North America, Europe, Middle East, Latin America
Notable Customers	Standard Bank, CAPITEC BANK, Chartway CREDIT UNION



(1) Link

Entersekt's Strategy

Strategy	Exceptional	**Entersekt is primarily an authentication player through a robust platform solution – their solution can be leveraged by financial services to leverage risk-based authentication for ATO prevention.**
Behavioral Capabilities	Exceptional	Entersekt offers protection against ATO attacks through its robust behavioral capabilities which include behavioral biometrics, behavioral analytics, as well as bot detection to inform its analysis and prevention of fraud.
Passwordless Authentication	Exceptional	The company's platform-agnostic approach supports various passwordless methods, including biometrics like fingerprints and facial scans, FIDO2-aligned authentication and passkeys, providing financial institutions with a highly secure alternative to traditional password-based systems.
Cost	Exceptional	Entersekt's pricing model is primarily subscription-based, tailored to the specific needs and deployment options of each client. The company offers customizable solutions across various channels and devices
User Experience	Exceptional	The company supports a strong user experience by offering a single-unified authentication platform that leverages its proprietary Context Aware™ Authentication to create personalized, frictionless experiences while maintaining high-security standards. This ultimately reduces frustration and cart abandonment for financial institutions and their customers.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Strategy

Entersekt's platform solution takes a comprehensive approach to authentication, leveraging various advanced capabilities to provide secure and frictionless experiences across multiple channels. The platform incorporates behavioral analytics to analyze user behaviors, device interactions, and transaction patterns, enabling the identification of anomalies that may indicate fraudulent activities. Additionally, Entersekt's solutions leverage behavioral biometrics, which involves analyzing unique user characteristics such as typing patterns, swipe gestures, and device movements to create comprehensive user profiles and detect deviations from expected behavior.

Entersekt's platform supports various passwordless authentication methods, including biometrics (facial recognition, fingerprint, and voice recognition), mobile authenticators, and industry standards like FIDO Authentication. These passwordless capabilities enable financial institutions to reduce reliance on traditional passwords, enhance security, and provide seamless user experiences across multiple channels, such as mobile banking apps, online banking, and digital payments.

Entersekt's focus on providing a secure SaaS platform suggests a subscription-based pricing model. Additionally, the emphasis on delivering measurable ROI, such as higher transaction success rates, reduced fraud losses, and cost savings through streamlined authentication processes, indicates that the commercial model may be tailored to individual customer needs and aligned with the platform's ability to drive tangible business benefits.

Entersekt's Market Presence

Market Presence	Excellent	**Entersekt demonstrates a strong vertical focus in financial services with its authentication and payment security capabilities. They are well positioned to secure additional customers.**
Brand Awareness	Excellent	As a prominent player in authentication, about 61% of surveyed financial institutions recognize Entersekt and their solutions for consumer account takeover prevention. Entersekt's solutions exclusively focus on supporting financial institutions mitigate fraud risk.
Market Leadership	Excellent	Entersekt's financial authentication solution was recognized by 24% of banking respondents as being market-leading. Entersekt should consider leveraging additional fraud detection and prevention capabilities to boost its market leadership score for account takeover prevention.
Market Penetration	Excellent	By pursuing channel partner strategies with Mastercard and Q2, Entersekt has facilitated user growth, with over 200 million users leveraging its software. The company also has a specific vertical focus in financial services and is, therefore, well-penetrated.
Company Size	Excellent	As of May 2024, Entersekt has 300+ employees in offices in 23 countries worldwide, with a concentration in South Africa, the US, central Europe, and northern Europe. Its size positions the company between emerging players and industry incumbents.
Employee Growth	Strong	Following the acquisition of Modirum in December 2023, Entersekt retained much of Modrium team and, subsequently, experienced a period of employee growth of around 14% YoY.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Market Presence

Entersekt has solidified its position as a global leader in transaction authentication solutions for financial fraud prevention. The company has experienced significant revenue and customer acquisition growth, fueled by its continued expansion in the United States market and strategic partnerships. Since receiving an investment from Accel-KKR, a prominent Silicon Valley-based private equity firm, in fiscal 2022, Entersekt has witnessed a rapid acceleration of its business outside of South Africa. In fiscal 2023 alone, the company's contracted annual recurring revenue increased by an impressive 191%, while its US-based customer base grew by nearly 220%.

Entersekt's market presence extends across the United States, Europe, and Africa, where it has established a strong track record of working with leading financial services institutions over the past decade. The company's patented security innovations, including its Context-Aware Authentication technology, have positioned Entersekt as a global industry leader in authentication.

In 2023, Entersekt acquired Modirum 3-D Secure Payment Solutions. Entersekt added Modirum's 3DS solutions to its Entersekt Secure Platform for transaction authentication, and the Modirum 3DS team joined the company. The acquisition accelerates product development, expands Entersekt's existing product offering, and bolsters the company's ability to scale and support global customers. Modirum also brings an impressive list of customers that increases Entersekt's market share of financial institutions offering 3-D Secure.

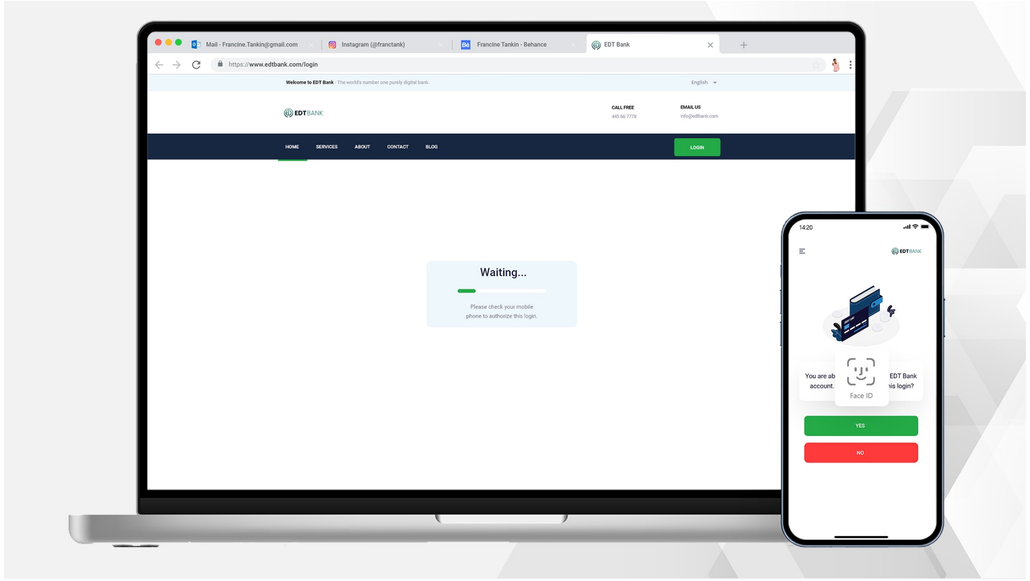
Entersekt Authentication

Entersekt Authentication offers a unified authentication platform for all company channels, such as mobile network operators (MNOs), browser, and mobile device. The product features multi-factor authentication (MFA), biometric authentication, and incorporates risk scoring models using multiple device signals, creating a comprehensive solution for protecting against account takeover (ATO).

ATO Prevention Product Capability Coverage[1]	
H App-Based Authentication	M Proxy and VPN Detection
H Biometric Authentication	M SIM Swap Detection
H Continuous Authentication	M Time-Based One-Time Passcode
H Data Breach Monitoring	L Behavioral Analytics
H Email-based One Time Passcode	L Bot Detection
H SMS / Phone One-Time Passcode (SMS OTP)	L FIDO2 Authentication
H Social Engineering and Scam Detection	L Knowledge-Based Authentication
M Behavioral Biometrics	L Magic Links
M Device Risk Scoring	L Signal Sharing Network
M Location Intelligence	L User Risk Scoring

H High Demand M Medium Demand L Low Demand

Product Visuals[2]



(1) Please see appendix for further information regarding Liminal's data acquisition and analysis methodology
(2) Product visuals sourced from the company.

Entersekt Banking Authentication

Product	Exceptional	Entersekt offers a complete set of tools for ATO prevention, featuring customizable options for both fraud detection and authentication.
Product Capability	Exceptional	Entersekt's product capability suite integrates both authentication and fraud signals, including biometric authentication and social engineering scam detection. This comprehensive approach makes it one of the most complete solutions among all benchmarked vendors.
Scalability	Excellent	Focusing exclusively on financial services, Entersekt has demonstrated its ability to support organizations as they scale, securing more than 2.5B transactions in the last year.
Customization	Excellent	Entersekt customers can create seamless experiences with step-up authentication that assesses risk levels based on user actions and contextual data, aligning with the preferences of financial institutions.
Accuracy	Strong	Entersekt's authentication accuracy rates are lower compared to other vendors we've benchmarked. However, its extensive product suite ensures robust coverage across the entire customer lifecycle, providing strong protection for various stages of user interaction.
Product Integration	Excellent	As an all-in-one platform, Entersekt allows customers to access all its services through a single integration, providing a wide range of highly demanded capabilities.
Buyer Satisfaction	Excellent	Entersekt employs a variety of signals and silent authenticators for comprehensive threat detection. By offering a wide range of MFA methods, the company meets buyers' specific needs, ensuring tailored security solutions.

Note: The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of *only* leading vendors for ATO prevention vendors. Vendors outside the scoring buckets are not considered leading ATO prevention vendors.

Analyst Notes on Entersekt Banking Authentication

Entersekt provides financial institutions with a secure, cross-channel authentication platform that addresses financial fraud prevention, account takeover schemes, and seamless user experiences. At its core is the patented Context Aware™ Authentication technology, which considers factors like transaction context, risk signals, and customer preferences to determine the best authentication method in real time. This technology enables a unified authentication strategy across online banking, in-branch services, call centers, digital payments, and open banking channels.

The platform includes mobile, MNO, and browser authentication to protect customers from digital fraud and identity theft. It also offers 3D Secure solutions for low-friction payment authentication and secure cashless payment experiences. Entersekt enhances fraud prevention, customer experiences, transaction success rates, and compliance with regulations by migrating its customers to a SaaS model and focusing on API-based capabilities. The company is developing deployment packages to streamline specific use cases such as login, account recovery, and identity verification.

Liminal™ | link™ by Liminal

LINK INDEX

Survey Results

Market Demand Survey Results Overview

We conducted outreach to banking customers who leverage ATO prevention solutions.

Our survey[1] reached 50 leading professionals in the identity and fraud space as respondents. We received significant participation from representatives of large enterprises with extensive global customer reach and gathered responses from various functional roles within each organization.

According to our survey findings, we've collected valuable insights to grasp the market's demand for ATO prevention solutions.

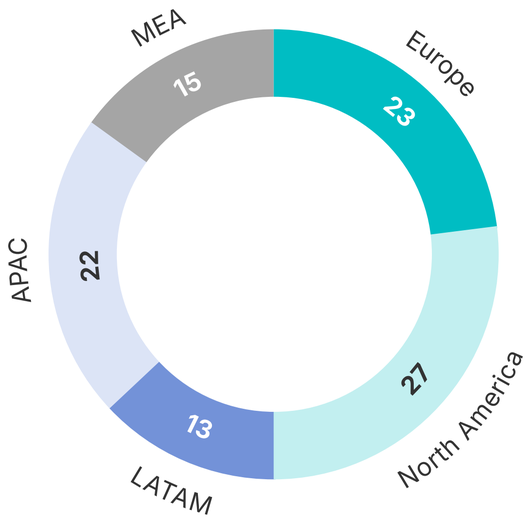
(1) All results referred to below are sourced from ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Survey Demographics: Buyer Profile

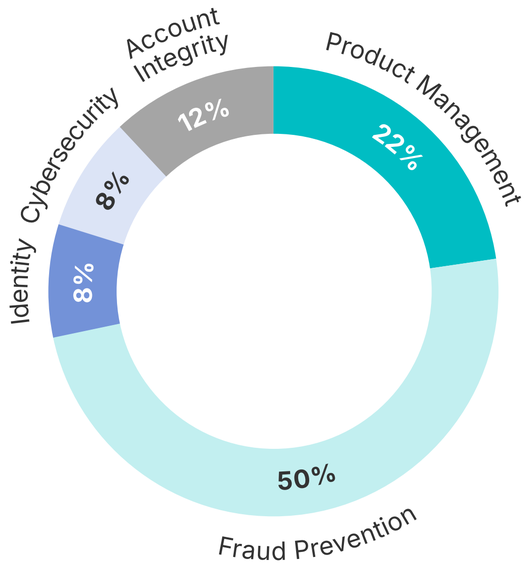
Our survey had a global set of respondents from several geographies, functional areas, and company sizes who are current solution seekers of ATO prevention solutions.

Survey Respondent Demographics (N = 50)

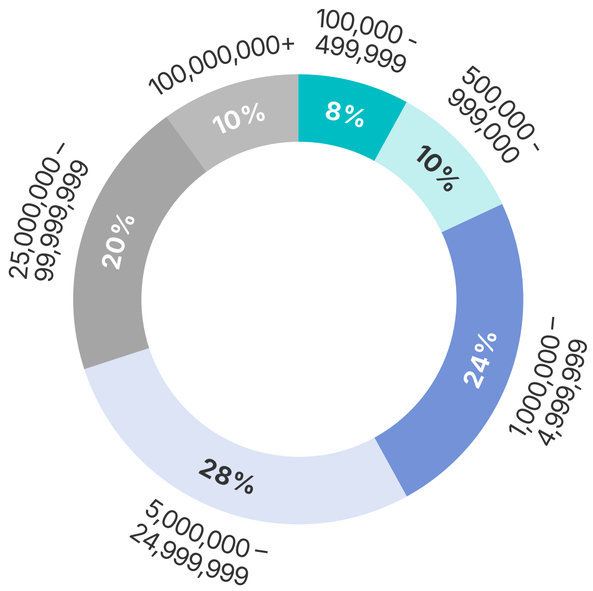
Geography
(By Region[1])



Functional Area
(By Department)



User Count

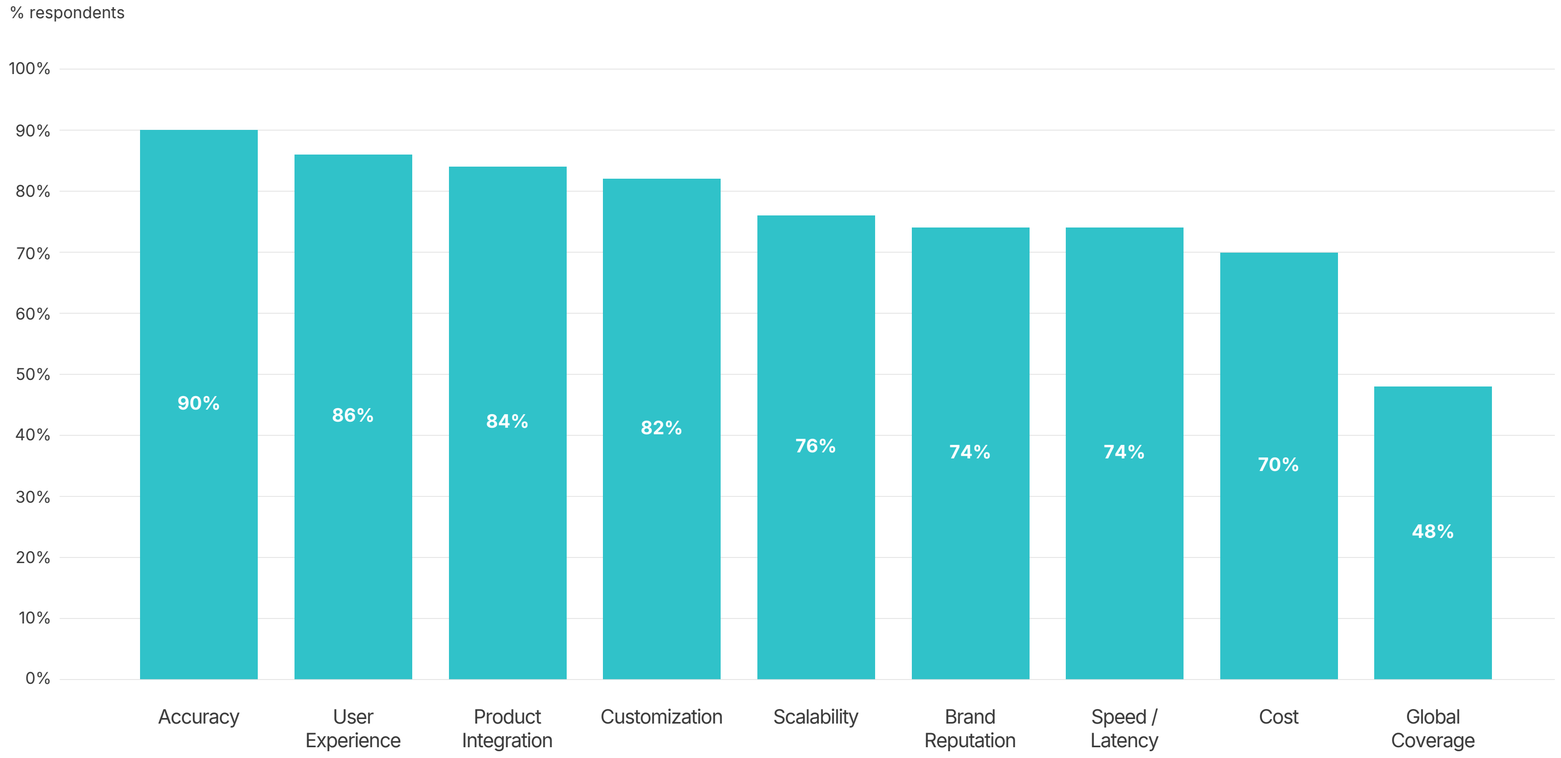


(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Top KPCs include accuracy, user experience, product integration, and customization for ATO prevention in banking

Key Purchasing Criteria for ATO Prevention Solutions in Banking

How would you prioritize the key purchasing criteria for ATO solutions?



(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

Accuracy (90%), user experience (86%), product integration (84%), customization (82%) are the most important key purchasing criteria for ATO prevention in banking.

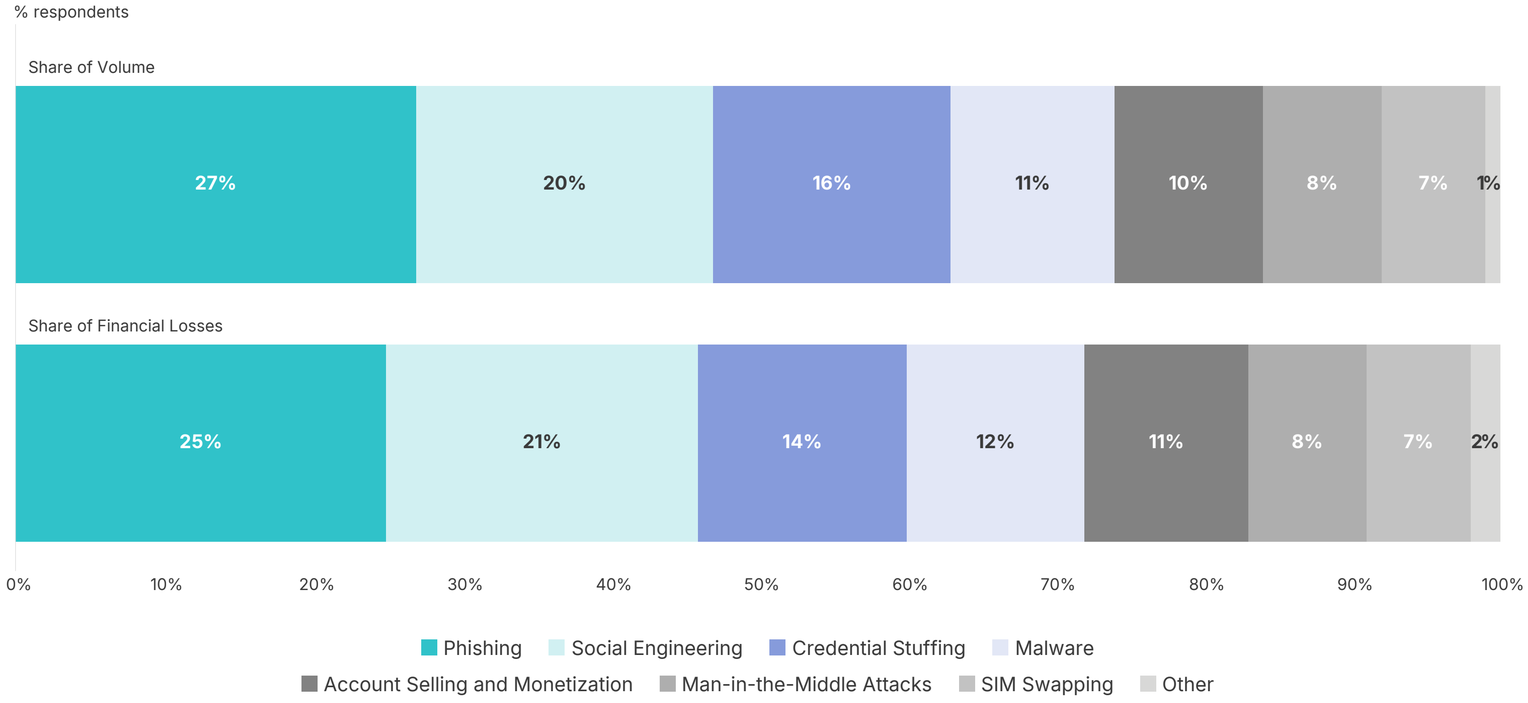
Banks prioritize accurate, user-friendly, and easily implementable customizable solutions.

Interestingly, global coverage, cost, and speed performed the weakest among our proposed key purchasing criteria. This suggests our buyers face highly localized and expensive problems, that are not addressed though maximizing efficiency but rather by optimizing for effectiveness.

Phishing and social engineering are the top ATO threat vectors

ATO Attack Vectors by Share of Financial Losses and Share of Total Volume[1]

What percentage of total ATO attack volumes are made up of the following threat vectors?
What percentage of financial losses from ATO attacks are made up of the following threat vectors?



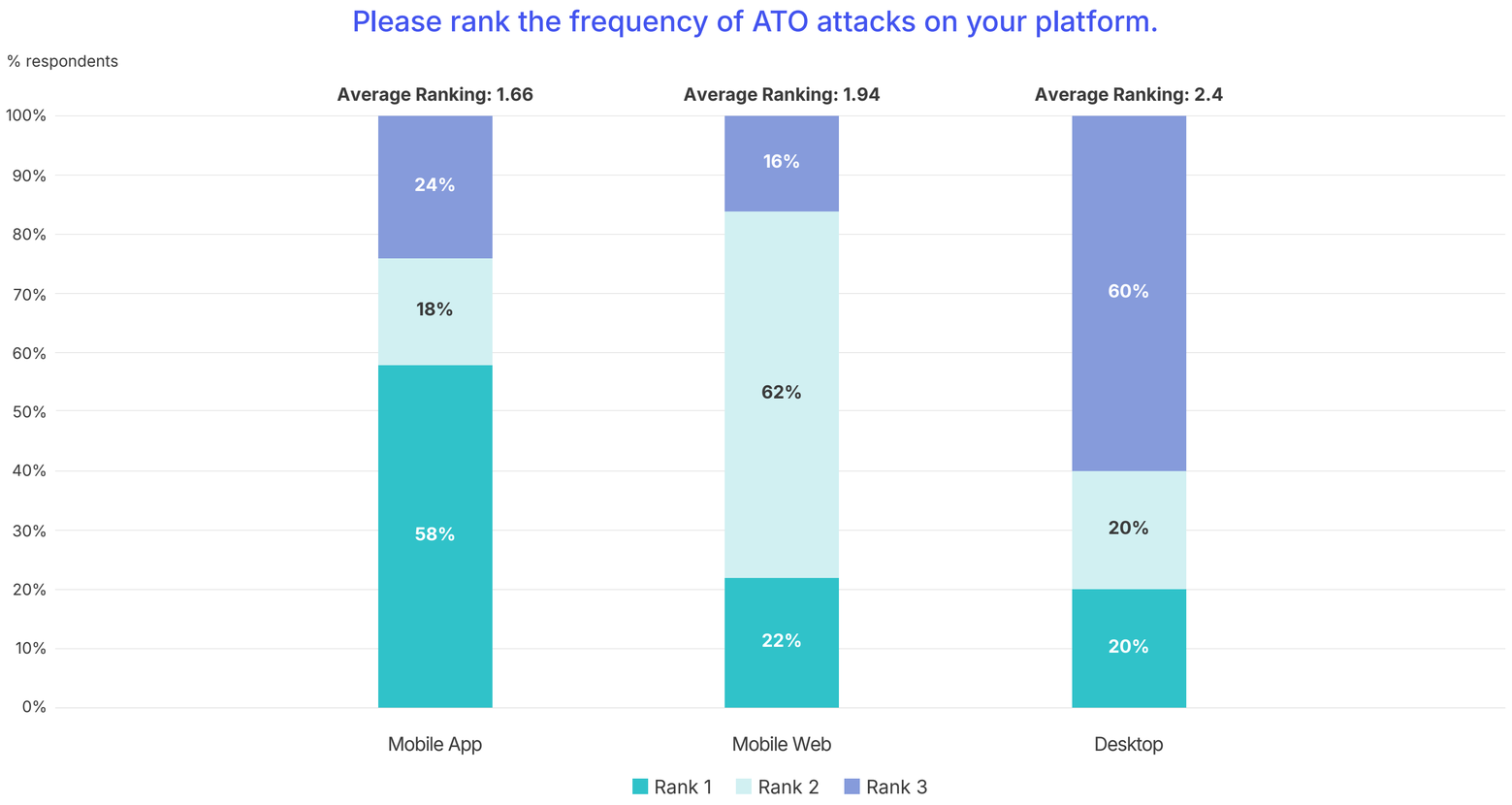
Phishing and social engineering are the biggest ATO threat vectors in terms of financial losses and total volume, with credential stuffing, account selling and monetization, and man-in-the-middle attacks following behind.

Phishing and social engineering are becoming more sophisticated as generative AI tools aid fraudsters to increase the scale and sophistication of attacks.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

ATO attacks predominantly occur via mobile app and mobile web rather than on desktop platforms

Frequency of ATO Attacks by Mobile App, Mobile Web, and Desktop[1]



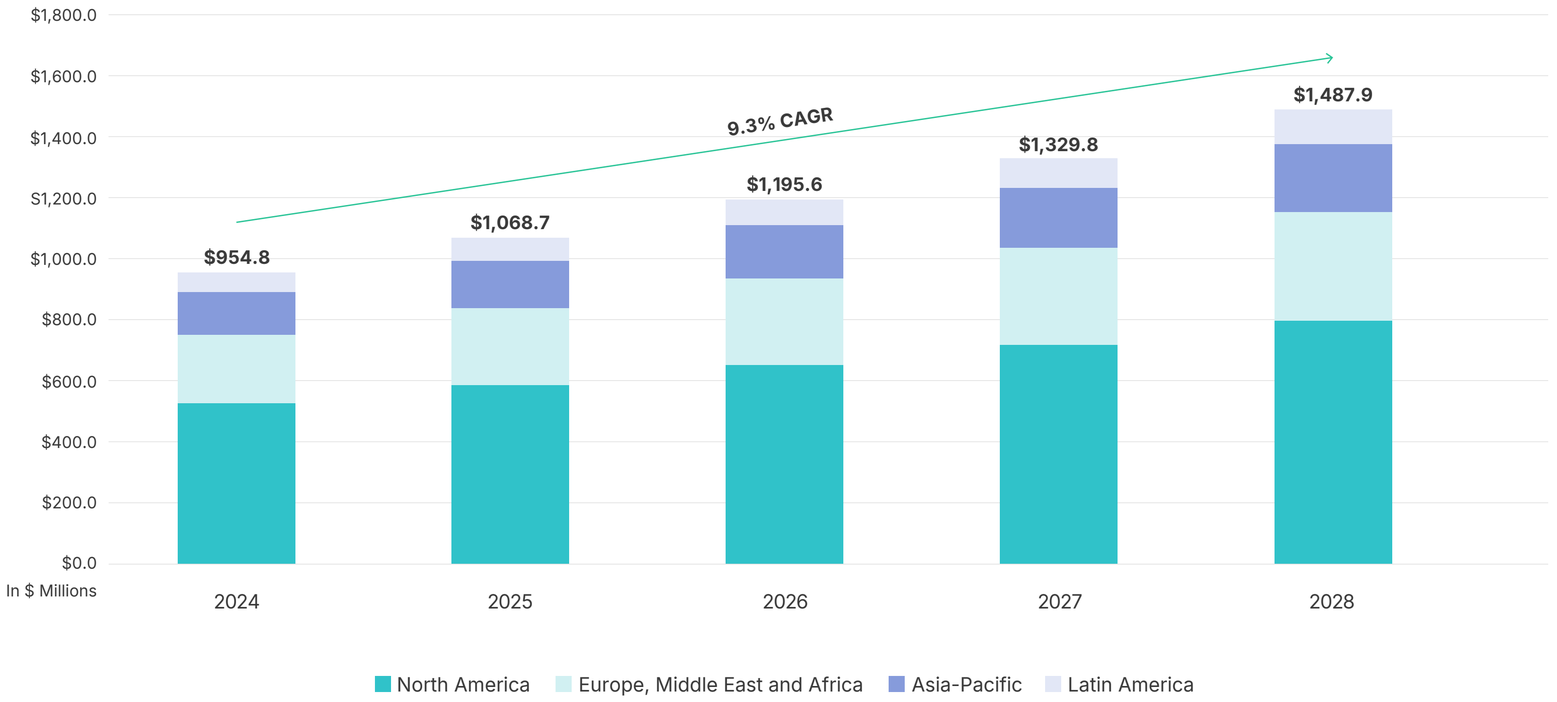
Mobile applications and mobile websites see more ATO attacks than desktop web channels, suggesting that fraudsters are prioritizing mobile channels.

Despite the outsized prevalence of mobile ATO attacks, only 44% of respondents report using mobile device signals as part of their ATO defense strategies, indicating a gap in prevention controls.

(1) ATO Prevention in Banking Buyer Survey, March 2024 (N=50)

There is a large and growing total addressable market (TAM) for ATO prevention solutions

Market Size for ATO Prevention Solutions in Banking[1]



The global TAM for ATO prevention in banking is projected to grow from about $954.8 million in 2024 to $1.5 billion by 2028, with a compound annual growth rate (CAGR) of 9.3%.[1]

We expect that demand for solutions will persist as banks aim to combat increasing levels of ATO fraud across various regions.

(1) Liminal's proprietary market sizing model, bottom-up approach building off of datasets on individual banks along with growth trends by geography, sector and other factors.

Liminal™ | link™ by Liminal

LINK INDEX

Appendix

Product Capabilities Definitions: High Demand

Demand	Product Capabilities	Definition
H	App-based Authentication	Biometric authentication is a process that verifies a user's identity using unique biological traits such as fingerprints, voices, retinas, and facial features.
H	Biometric Authentication	Biometric authentication is a process that verifies a user's identity using unique biological traits such as fingerprints, voices, retinas, and facial features.
H	Continuous Authentication	Continuous authentication is a security approach that verifies a user's identity throughout a session rather than just at the login point.
H	Data Breach Monitoring	Data breach monitoring is a threat detection capability that alerts users when one of their accounts and associated data has been leaked in a data breach. It involves tracking compromised personal information on the dark web and other illicit platforms to prevent identity theft.
H	Email-based One-Time Passcode	An email-based one-time passcode (OTP) is a form of authentication where a unique, temporary code is sent to a user's email address, which they must enter to gain access to a system or service. This code is valid for only one transaction or login session, making it more secure than a static password that could be reused or compromised.
H	SMS / Phone One-Time Passcode (SMS OTP)	SMS OTP (Short Message Service One-Time Password) is a form of two-factor authentication (2FA) that enhances security by sending a unique, automatically generated numeric or alphanumeric string of characters to a user's mobile device via text message.
H	Social Engineering and Scam Detection	Social engineering and scam detection involves rules-based or machine-learning models configured to identify customer behavior indicative of social engineering. Social engineering involves manipulating individuals to divulge sensitive information or perform actions that aid fraudsters in gaining unauthorized access to data or systems. Scam detection refers to identifying and preventing fraudulent schemes to deceive individuals into providing personal information or financial assets.

H High Demand

Product Capabilities Definitions: Medium Demand

Demand	Product Capabilities	Definition
M	Behavioral Biometrics	Behavioral biometrics identifies individuals based on their unique behavior patterns, particularly in human-computer interaction. Unlike physical biometrics, which rely on innate physical characteristics like fingerprints or iris patterns, behavioral biometrics focuses on patterns that emerge from a person's natural interactions and activities, such as typing rhythm, mouse movements, gait, and voice dynamics.
M	Device Risk Scoring	Device risk scoring is a subcategory of risk scoring that assesses the trustworthiness of a device. By analyzing various factors related to the device, such as IP address, device fingerprint, and location, businesses can assign risk scores to transactions or users, enabling them to make informed decisions on whether to approve, review, or reject transactions based on the likelihood of fraud.
M	Location Intelligence	Location intelligence leverages geolocation data to understand user behavior, deliver personalized services, and enhance marketing strategies based on real-time location information.
M	Proxy And VPN Detection	Proxy and VPN Detection refers to the methods and technologies used to identify whether a user connects to a service or network through a proxy server or a Virtual Private Network (VPN).
M	SIM Swap Detection	SIM Swap Detection is a security process used to identify and prevent SIM swap fraud, a type of identity theft where a fraudster manages to transfer a victim's phone number to a new SIM card they control.
M	Time-based One-Time Passcode (TOTP)	A time-based one-time passcode (TOTP) is an algorithmically generated temporary passcode, most commonly used as a secondary factor for multi-factor authentication. TOTPs can be generated by dedicated hardware tokens, websites, or mobile applications.

M Medium Demand

Product Capabilities Definitions: Low Demand

Demand	Product Capabilities	Definition
L	Behavior Analytics	Behavioral analytics is a data analysis process focusing on understanding how users interact with systems and applications to detect unusual behaviors that may indicate security threats or unauthorized activities. It tracks and analyzes a wide range of user activities - from account creation and form submissions to purchasing behavior - to glean insights into user preferences, habits, and intentions.
L	Bot Detection	Bot detection involves identifying entities or individuals that mimic user behavior, such as bots, malware, or rogue applications. These may evade traditional security tools by blending with regular user activities like browsing the web or sending emails. It also refers to analyzing traffic to a website, mobile application, or API to detect and block malicious bots.
L	FIDO2 Authentication	FIDO2 is an open authentication standard developed by the FIDO Alliance, an industry standards association dedicated to addressing the limitations of traditional password-based authentication. FIDO2 authentication utilizes device-stored credentials that are immune from phishing and brute-force attacks.
L	Knowledge-Based Authentication	Knowledge-based authentication (KBA) is used for identity verification by asking personal questions about the account owner. (e.g., “What was the name of your first pet?”)
L	Magic Links	Magic links are a one-time use link sent to the customer during the authentication process, enabling passwordless authentication.
L	Signal Sharing Network	Signal-sharing networks (or consortiums) are collaborative platforms where businesses share real-time fraud risk signals and intelligence to enhance fraud prevention strategies. These networks enable communication between organizations to share information regarding trusted users and bad actors.
L	User Risk Scoring	User risk scoring in fraud detection is a critical tool that evaluates the likelihood of a user’s behavior indicative of fraudulent activity. This process involves analyzing various data points and behaviors, such as transaction history, login patterns, and device usage, to assign a risk score to each user.

L Low Demand

Passwordless Feature Definitions

Product Capabilities	Definition
Device Based / Cloud Based Passkeys	Device-Based Passkeys are stored locally on a user's device and use biometric or PIN-based authentication, eliminating the need for passwords. Cloud-Based Passkeys are stored in the cloud, enabling synchronization and access across multiple devices with protection through multi-factor authentication.
QR Code Authentication	QR Code Authentication is a method where users scan a QR code with their mobile device to authenticate and gain access to an account or service, typically leveraging the camera and secure apps for verification.
WebAuthn	WebAuthn is a web standard that enables secure, passwordless authentication using public key cryptography, allowing users to log in to online services security keys or other authenticators.

Exceptional, Excellent, Strong Scoring Buckets Definitions

Scoring Buckets	Definition
Exceptional	Vendors in this category represent the pinnacle of performance in the market and are in the top quartile among leading vendors for specific criteria. They not only meet all industry standards but also significantly exceed them. Exceptional vendors demonstrate advanced technological capabilities, comprehensive coverage, innovative solutions, and extraordinary customer service.
Excellent	Vendors rated as excellent provide very strong services that go beyond the basic fulfillment of criteria and are in the second quartile among leading profiles for specific criteria. They showcase high levels of proficiency and reliability in their solutions and customer support. These vendors are recognized for their robust feature sets, comprehensive integrations, and effective detection and reporting capabilities. While they may not reach the pinnacle of the Exceptional category, their performance significantly enhances customer authentication processes.
Strong	Vendors classified as strong adequately meet the established criteria necessary for effective customer authentication and are in the fourth quartile among top vendors (though perform better than vendors who did not make our final list). They provide solid, dependable technology and support. These vendors offer functional and effective solutions that satisfy basic requirements for authentication and risk detection. While they may lack the cutting-edge features of higher-ranked vendors, their services are competent and reliable for organizations looking to authenticate their customers.

Link Index Methodology: Product

Product Criteria	Weighting	Definition	Why It Matters
Product Capability	40.0%	The completeness of a vendor's product capabilities at solving ATO prevention in banking based on buyer demand.	Companies with more in-demand product capabilities are better at solving ATO prevention.
Buyer Satisfaction	15.0%	How satisfied customers report being when using a specific vendor.	A vendor who satisfies its customers is more likely to retain and increase their customer base.
Accuracy	17.5%	The ability to identify bad actors with high effectiveness.	Accurate solutions effectively decrease the amount of fraud losses without false positives.
Product Integration	10.0%	How easy a solution is to deploy / integrate for buyers.	Solutions that are easy to implement can be more easily adopted and will be able to capture more of the market.
Customization	10.0%	The degree of customization available in a solution, such as adjusting risk-scoring models, configuring rules, and setting up alerts/notifications.	Banks want to be able to fine tune ATO solutions to most effectively cater to their risk posture and customer flows to effectively provide security while limiting friction.
Scalability	7.5%	The ability to defend against high volumes of ATO attempts while maintaining effectiveness.	Vendors with scalable solutions will be able to capture bigger customers and, therefore, service more of the market.

Link Index Methodology: Strategy

Product Criteria	Weighting	Definition	Why It Matters
User Experience	30.0%	The ability of a vendor to provide ATO protection while also ensuring a seamless user experience for consumers.	Banking users want to feel like their account is adequately protected while avoiding considerable friction.
Cost	25.0%	The ability to offer cost-effective solutions for ATO prevention in banking.	Banks want to find highly effective solutions but also want to stay within budget.
Behavioral Capabilities	25.0%	Behavioral signals refer to patterns and characteristics of user behavior that are monitored and analyzed to detect fraudulent activities. Vendors with strong behavioral capabilities offer capabilities such as behavioral biometrics, behavioral analytics, and bot detection.	Behavioral signals provide highly sophisticated fraud detection leveraging passive signals, ensuring strong user experience paired security.
Passwordless Authentication	20.0%	Passwordless Authentication is a method of verifying a user without requiring a traditional password, instead relying on alternative methods. Vendors with passwordless authentication offer WebAuthn, QR code authentication, and device-based / code-based passkeys for ATO prevention.	Passwordless Authentication is a method of verifying a user without requiring a traditional password, instead relying on alternative methods.

Link Index Methodology: Market Presence

Market Criteria	Weighting	Definition	Why It Matters
Brand Awareness	25.0%	The amount of buyers that are aware of a vendor.	Well-known vendors are better suited to capture more market share.
Market Leadership	30.0%	The number of buyers who believe this vendor is a market leader.	Vendors known as market leaders are better suited to capture more market share.
Market Penetration	25.0%	The share of the market that uses a particular vendor.	Vendors that process large numbers of transactions for large clients will yield higher market penetration
Company Size	10.0%	The total employee headcount of a company.	A large company has the stability and bandwidth to take on bigger clients and drive larger revenues.
Employee Growth	10.0%	How fast a company's employee count is growing (YoY).	A growing company means it has strong prospects for revenue growth and will be a more formidable player in the market.

ROI Calculations

Reduction in Fraud Losses

Metric	Value	Source
Number of successful fraud incidents using poor solution	133,633.33	Buyer Demand Survey
% of successful fraud incidents related to ATO	33.50%	Buyer Demand Survey - weighted average
Number of ATO incidents using poor solution	44,767	Calculation
Average loss per ATO incident using poor solution	$13,400.00	Buyer Demand Survey
Poor solution fraud losses	$599,880,033.33	Calculation
Average customer base of those using a poor solution	36,700,000	Buyer Demand Survey
Average fraud loss per customer	$16.35	Calculation
Number of successful fraud incidents using strong solution	76,913.65	Buyer Demand Survey
% of successful fraud incidents related to ATO	20.94%	Buyer Demand Survey - weighted average
Number of ATO incidents using strong solution	16,109	Calculation
Average loss per ATO incident using strong solution	$6,430.50	Buyer Demand Survey
Strong solution fraud losses	$103,589,797.00	Buyer Demand Survey
Average customer base of those using a poor solution	26,498,889	Buyer Demand Survey
Average fraud loss per customer	$3.91	Calculation
Reduction in Fraud Losses per Customer	**$12.44**	**Calculation**

Reduction of Operation Costs

Metric	Value	Source
Total number of employees required per ATO with poor solution	3	Assumption
Employee time (hours) spent per ATO with poor solution	6.10	Buyer Demand Survey
Cost of employee per hour	$21.29	Indeed
Total cost of team using a poor solution	$389.61	Calculation
Total number of employees required per ATO with strong solution	3	Assumption
Employee time (hours) spent per ATO with strong solution	5.69	Buyer Demand Survey
Cost of employee per hour	$21.29	Indeed
Total cost of team using a strong solution	$363.65	Calculation
Reduction of Operational Costs with a Strong Solution	**$25.96**	**Calculation**

Customer Retention Savings

Metric	Value	Source
% of customer abandonment poor solution	19.80%	Buyer Demand Survey
% of customer abandonment good solution	15.14%	Buyer Demand Survey
Average customer lifetime value	$4,500	Forbes
Customer base	1	Placeholder number
Customer Retention Savings per Customer	**$210**	**Calculation**

Liminal™ | link™ by Liminal

Actionable Market Intelligence

Link

Through our proprietary database, Link, we monitor thousands of companies and products across the digital landscape. Our insights allow us to predict and understand trends before they happen.
Paid and free access options available.

- Specialized Data on Companies, Products, Regulations, and more
- Market and Buyer's Guides
- Benchmarking Reports
- Outside-in Research
- Market Sizing
- Competitive Battlecards

Membership

Liminal is your trusted partner. As a member, you have unparalleled access to our team and extended network of industry experts. Our deep domain experience provides us with the ability to remain on-call and to provide you with market intelligence when opportunity strikes.

- Analyst Access
- Executive Summits
- Private Events
- Expert Network
- Virtual Workshops
- Ad hoc Support

Advisory

We advise the world's most innovative leaders on building, buying, and investing in the next generation of integrated digital identity technologies.

- Market Intelligence
- Business and Corporate Strategy
- M&A and Commercial Due Diligence

www.liminal.co | **www.liminal.co/linkplatform**

Liminal Strategy, Inc.
825 Third Avenue, Suite 1700, New York, NY 10022

www.liminal.co | info@liminal.co