Liminal Research Report | May 2024

Account Takeover Prevention in Banking

● Market and Buyer's Guide

Liminal™

Contributors

Travis Jarae
CEO

Will Charnley
Managing Director

Cameron D'Ambrosi
Senior Principal

Coleston Smith
Analyst

Jennie Berry
President

Stacy Schulman
Chief Marketing Officer

Jonathan Gergis
Associate

Zita Jameson
Analyst

Table of Contents

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

Key Takeaways

Account takeover (ATO) involves a bad actor gaining access to and control over a user's account. Once access is secured, the bad actor can misuse the account for various illegal activities, including stealing funds and making unauthorized purchases. Typically initiated through phishing, malware, or exploiting credentials from data breaches, the consequences of ATO are severe, resulting in significant financial loss. The banking industry employs ATO prevention solutions to safeguard customers and themselves from losses due to unauthorized account access. Presently, these institutions rely on various solution providers to mitigate a broad spectrum of threats. To delve deeper into these issues, we surveyed 50 technology purchasers at banks across five regions: North America, Europe, Latin America, Asia Pacific, the Middle East and Africa.

- **Mobile channels are the primary source of ATO attacks, yet only a minority of banks rely on mobile device signals.** Mobile channels have become the primary targets for ATO attacks across banks. Mobile apps and web interfaces are more frequently compromised than desktop interfaces. Despite the increasing threat, only 44.0% of banks incorporate mobile device signals into their ATO defense strategies, indicating a significant delay in responding to mobile vulnerabilities.[1]

- **Customized solutions are necessary to respond to regional privacy laws.** Banks are concerned about the challenges in data collection due to regulations, with 96.0% worrying about balancing ATO prevention with privacy laws. Moreover, 82.0% reported that some customization was necessary to comply with regional regulations.[1]

- **Banks expect data restrictions to make their ATO solutions less effective.** Banks are concerned that restrictions on fraud detection signals by Big Tech companies like Apple and Google may significantly undermine their efforts to prevent ATO incidents. Around 96.0% of banks are worried about limitations on device signals, while 90.0% are concerned about other data restrictions, such as those placed on Chrome cookies.[1]

- **The Total Addressable Market (TAM) for ATO prevention solutions in banking is large and growing.** As digital banking becomes more popular and threats become more sophisticated, we expect banks to increase their investment in ATO prevention significantly. This surge in spending is driven by the need to protect sensitive financial information and enhance customer security. Liminal outlines the market's potential and driving forces, including an estimation of the global TAM for ATO prevention in banking, which 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%.[2]

Introduction

Account Takeover (ATO) is when a bad actor gains unauthorized access and control of a user's account, such as banking, e-commerce, or social media account. Once access is obtained, the attacker can exploit the account for various malicious activities, including stealing funds, making unauthorized purchases, or gaining further access to other accounts through reset links or saved credentials. The process often begins with techniques such as phishing, malware, or using credentials exposed in data breaches. The impact of ATO can be severe, leading to financial loss and damaging the victim's credit score and personal reputation.

ATO attacks are particularly alarming at banks because they provide direct access to financial assets and personal data, making the industry more susceptible to such incidents than others. The methods used in ATO attacks on banks are becoming increasingly sophisticated, resulting in financial losses and eroding trust in financial institutions. Specifically, the average fraud loss associated with a successful ATO attack is $6,232.[1] Therefore, it is crucial to implement advanced security measures to combat these attacks.

The vendors specializing in preventing ATO for financial institutions are primarily built with product capabilities in the Authentication and Fraud Detection and Prevention solution segments of the Liminal Landscape. While fraud prevention remains a cat-and-mouse game, there are several product capabilities and features that fraud teams are finding success with. In particular, banking practitioners are interested in providers who offer app-based and biometric authentication, continuous authentication, data breach monitoring, social engineering and scam detection, and one-time password (OTP) solutions through SMS and email. The demand for reliable ATO prevention solutions is rising as fraudsters use sophisticated techniques leveraging AI/ML, enabling scalable attacks across a myriad of vectors. These attacks involve social engineering tactics such as phishing, vishing (via phone calls), and impersonation to trick online banking customers and employees. Fraud teams have reported a 66.8% increase in social engineering attacks in the past two years, indicating a growing threat.[1]

This report provides an in-depth exploration of the ATO prevention market for banks, offering a detailed overview that covers key aspects such as decision-making factors, purchasing criteria, and the unique needs of buyers looking to fend off attacks. It explores the offerings of notable solution providers while also analyzing the major types of ATO threats and their financial repercussions. Furthermore, it addresses the essential market demands, challenges, and concerns expressed by those searching for effective solutions. This research equips banks with the necessary knowledge to prepare for and mitigate the severe consequences of account takeovers by comprehensively examining the current strategies and technologies effective in thwarting ATO incidents.

Market Overview

Account Takeover Prevention Definition

ATO is a fraud attack where a third party gains unauthorized access to a user’s account and takes control of it. The attacker obtains sensitive information such as usernames, passwords, and other credentials through phishing, malware, data breaches, or social engineering tactics. Once they can access the account, they can perform fraudulent transactions, change account details, and even lock out the legitimate owner. ATO is a significant security threat, as it can lead to financial loss and damage to the user’s reputation and credit status. It differs from identity theft, which involves impersonating someone to open new accounts, while ATO focuses on taking over existing accounts.

In this research report, we distinguish between workforce and customer account takeovers. Workforce account takeovers refer to unauthorized access within an organizational context, where employee accounts are compromised to gain access to sensitive corporate information, internal systems, or infrastructure. The motivation behind such breaches can range from espionage to sabotage, requiring a security apparatus deeply integrated with corporate policies, access control mechanisms, and sophisticated IT defenses. While there is some overlap between customer account takeover and workforce account takeover, the threat vectors and solution strategies differ. Customer account takeover affects both businesses and customers, so we expect customer account takeover prevention solutions to be most relevant in preventing fraudulent behavior and minimizing risk.

Account Takeover Prevention in Banking

Account takeover attacks pose a significant threat to banks, primarily because of their direct access to financial assets and personal financial data, making them prime targets due to the high value of the accounts they manage and the extensive personal information they store. The incidence of fraud and scams, including ATO, is increasing alarmingly. In 2023, the Federal Trade Commission (FTC) reported a 14.0% increase in reported losses from the previous year.[3]

The methods used for ATO attacks across banks have evolved with recent technology, becoming more sophisticated and harder to detect. These methods can range from simple credential stuffing, where automated scripts are used to attempt access with stolen username-password pairs, to more complex man-in-the-middle attacks, where attackers intercept and manipulate communications between the user and the bank. Attackers who successfully takeover an account can execute unauthorized fund transfers, bill payments, or gather enough information to enable further fraudulent activities. The impacts extend beyond immediate financial loss, potentially undermining trust in financial institutions and the broader stability of the economic system.

Importance of Account Takeover Prevention Solutions

The need for robust protections against account takeover attacks is more pressing than ever. These attacks, growing in sophistication and frequency, result in substantial financial losses due to fraud. Increased computational power allows attackers to expand their operations and enhance the complexity of automated threats like credential stuffing and malware. Additionally, the advent of artificial intelligence and machine learning technologies enables adversaries to refine their strategies and exploit vulnerabilities more effectively. Generative AI technologies have further advanced phishing and social engineering tactics. For example, attackers can now employ tools like ChatGPT to craft highly personalized and convincing phishing emails, making these schemes more effective and realistic.

Platforms must prioritize robust account takeover prevention solutions to maintain user trust and prevent account abandonment. In today’s digital-first world, security is expected to be built-in, not optional. Inadequate security can drive customers away. A Vercara Research survey found that 66% of customers would lose trust in a company after a data breach, underscoring the need for effective security measures.[4] Banks face a particularly high risk; they could lose substantial revenue if security issues drive customers away. Industry experts estimate that the lifetime value of a banking customer ranges from $2,000 to $4,500.[5] Consequently, investing in effective account takeover prevention solutions can yield significant returns.

Top account takeover prevention solutions deploy a range of techniques to spot potentially risky activities. These methods include detecting bots, analyzing behavior, using behavioral biometrics, and employing various authentication strategies. By leveraging these tools, leading providers can block malicious entities at several points during a user’s lifecycle, protecting against financial losses. As criminals adopt new technologies to refine their strategies, solution providers respond with sophisticated AI and machine learning algorithms. These algorithms are equipped with self-learning features to identify unusual activities accurately. Additionally, these solutions strive to prevent fraud while ensuring a user-friendly experience, crucial for retaining users without driving them away. This outcome could prove more harmful than the fraud itself.

Authentication, Fraud Prevention, or Both?

Providers specializing in account takeover prevention employ various techniques that are also common in fraud detection and prevention, as well as in authentication solutions, according to the Liminal Landscape. They employ fraud indicators, such as user behavior, device characteristics, and geographical data, to identify potentially risky actions. To confirm identities on mobile devices, they implement authentication methods like SMS-based one-time passwords and app-based verification. However, it's important to recognize that not all authentication and fraud prevention features are specifically aimed at preventing account takeovers. For instance, some solutions include single sign-on and orchestration features that, while they support broader identity management for workforces and customers, are less pertinent to preventing account takeovers. Moreover, some fraud prevention solutions primarily focus on managing chargebacks, which are not directly related to stopping account takeovers.

Account Takeover Threat Vectors

- **Credential Stuffing:** Credential stuffing is when attackers use stolen login credentials to access multiple accounts on different platforms. This technique relies on people reusing their passwords across different platforms.
- **Phishing:** Phishing scams utilize various communication methods, such as email, text messages, and fake websites, to deceive individuals into revealing their login credentials by impersonating trustworthy entities.

- **SIM Swapping:** SIM swapping is a fraudulent technique that involves convincing a mobile carrier to transfer the victim’s phone number to a SIM card that the attacker controls. Once the attacker controls the phone number, they can intercept authentication codes, such as SMS OTP, which enables them to access secured accounts.

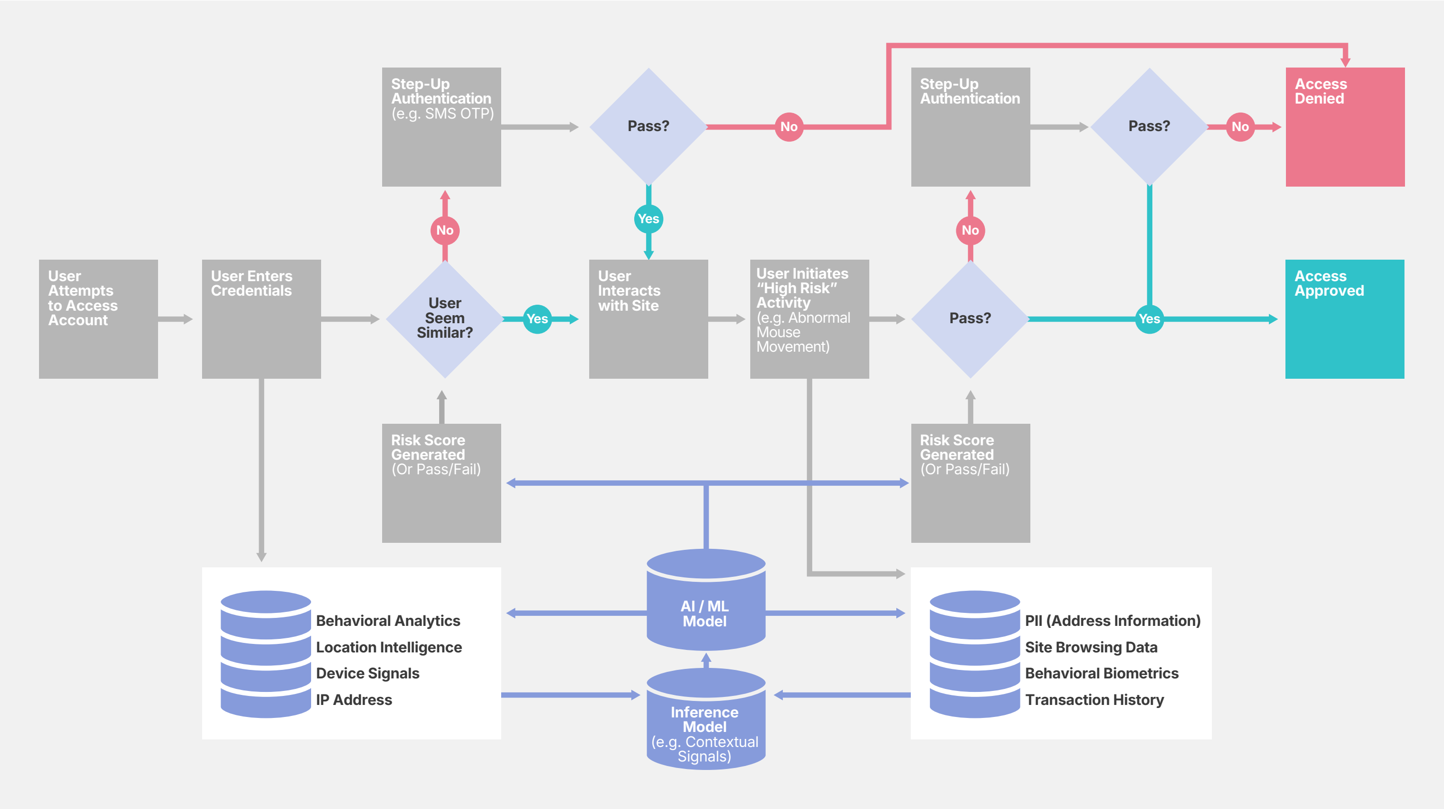
- **Malware:** Malware, such as Trojans or spyware, can obtain login credentials from user devices. Once installed, it can record keystrokes or manipulate legitimate banking apps to steal sensitive information.

- **Man-in-the-Middle (MitM) Attacks:** MitM attacks involve intercepting communication between two parties without their knowledge. Attackers capture sensitive information transmitted over unsecured or compromised networks.

- **Social Engineering:** Social engineering attacks leverage human psychology to extract sensitive information through methods such as pretexting, baiting, and quid pro quo schemes rather than exploiting technical vulnerabilities.

- **Account Selling and Monetization:** Once hackers gain access to an account, they can use it to their advantage. For instance, they may transfer money, make purchases, or sell the account credentials on the dark web. This is especially prevalent with accounts that store sensitive financial information or other valuable data.

Figure 1: Account Takeover Prevention Process Flow



Necessary Product Capabilities

Based on our survey, below are the most sought-after product capabilities for solving ATO fraud at a bank.[1] The following scale was used to prioritize product capabilities:

- **High Demand:** These capabilities are considered essential for solving the use case
- **Medium Demand:** Helpful capabilities, but not a requirement
- **Low Demand:** Capabilities that buyers do not prioritize

Table 1: Account Takeover Prevention Capabilities in Banking

Product Capabilities	Overall Demand
App-based Authentication	H
Biometric Authentication	H
Continuous Authentication	H
Data Breach Monitoring	H
Email-based One-Time Passcode	H
SMS / Phone One-Time Passcode (SMS OTP)	H
Social Engineering and Scam Detection	H
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
Behavioral Analytics	L
Bot Detection	L
FIDO2 Authentication	L
Knowledge-Based Authentication	L
Magic Links	L
Signal Sharing Network	L
User Risk Scoring	L

H High Demand

M Medium Demand

L Low Demand

Notable ATO Features

Highly Demanded Capabilities

Many highly demanded capabilities, such as app-based authentication, biometric authentication, continuous authentication, data breach monitoring, and email-based and SMS one-time passcodes, are expected to remain in high demand.

App-based Authentication

App-based authentication, which uses an authenticator app, is a powerful security measure to safeguard online accounts. This method employs multi-factor authentication (MFA), which requires a combination of a time-based, one-time passcode (TOTP or OTP) generated by the app and the usual login details like passwords to access accounts. One of the benefits of app-based authenticators is that they can work even without an internet connection, making it possible to generate codes offline. Moreover, they are more secure than SMS-based authentication methods, which are vulnerable to interception.

Biometric Authentication

Biometric authentication is a security method that uses unique biological traits of individuals to confirm their identities. This method involves comparing physical or behavioral characteristics, such as fingerprints, facial features, palm prints, voice patterns, and iris or retina patterns, to verified data stored in a database. By doing so, it ensures a 1:1 biometric matching process. This method is highly effective in protecting sensitive information due to the distinctiveness of biometric traits. However, securing this information is crucial as biometric data is permanent and cannot be reset like passwords, which can lead to misuse.

Continuous Authentication

Continuous authentication is a security approach that verifies the identity of a user dynamically throughout an active session instead of relying solely on the initial login credentials. This approach uses a combination of user behavior analytics and biometrics to ensure that the user interacting with the system is the legitimate account holder. Continuous authentication effectively prevents account takeover, offering a real-time defense mechanism against unauthorized access. By continuously monitoring and authenticating the user's identity, any deviation from the established behavior patterns can trigger alerts or automatic session termination, thwarting potential takeover attempts even after the initial breach and ensuring ongoing account security.

Data Breach Monitoring

Data breach monitoring is a capability that alerts users if their accounts and associated data are compromised in a data breach. It actively tracks potentially compromised personal information across the dark web and other unauthorized platforms to help prevent identity theft. Looking ahead, advancements in data breach monitoring are expected to include improved scanning technologies that can detect a wider variety of personal data types, the provision of real-time alerts for quicker responses, and integration with additional security measures such as identity theft insurance, offering more comprehensive protection against financial crime threats.

Email-based One-Time Passcode

Email-based one-time passcode (OTP) is a security method for sending a unique, temporary code to a user's email. This code must be entered to access a system, and it's only valid for a single transaction or session. It offers more security than a reusable static password, which makes it a popular method for protecting user accounts. However, retrieving OTPs from email can be inconvenient for users, and there is a risk of delays or codes expiring before use. Due to these limitations and vulnerabilities to attacks such as man-in-the-middle or email account breaches, there is a growing trend toward adopting more secure methods of delivering OTPs.

SMS / Phone One-Time Passcode (SMS OTP)

SMS OTP (Short Message Service One-Time Password) is a type of two-factor authentication (2FA) that adds an extra layer of security to user accounts. It sends a unique and automatically generated numeric or alphanumeric code to a user's mobile device through a text message. Many banking platforms and industries have adopted this method because it is easy to implement. However, despite its popularity, SMS OTP has been criticized for security weaknesses, including vulnerabilities to SIM swapping and phishing attacks. These concerns have prompted suggestions to explore alternative OTP delivery methods that offer enhanced security.

Emerging Capabilities

Some currently less popular capabilities like behavioral analytics, behavioral biometrics, bot detection, and FIDO2 authentication may increase demand. Despite their sophistication and current lower levels of adoption, these technologies will likely become more popular as banks continue advancing their fraud detection and authentication programs.

Behavioral Analytics

Behavioral analytics analyzes human behavior through data gathered from various digital platforms, such as websites, mobile applications, sensors, and social media. This approach utilizes indicators like keystroke patterns, touchscreen interactions, mouse movements, device orientation, and walking patterns to identify potentially risky behaviors. Analyzing user behavior in context helps distinguish between legitimate users and potential threats. One of the essential features of behavioral analytics is that banks can implement it instantly without relying on historical session data to be effective.

Behavioral Biometrics

Behavioral biometrics is a field that involves the study and analysis of an individual's unique behavioral patterns. This includes signals such as typing rhythm, mouse movement, and touchscreen behavior, which authenticate a user's identity. Combining these signals creates a unique user profile across multiple sessions, which is used as a baseline for comparison in subsequent sessions. Behavioral biometrics solutions typically require approximately 15 user interactions to establish a reliable user profile. Sessions to operate optimally, once up and running, the solution proves to be highly effective in detecting risks.

Bot Detection

Bot detection is the process of identifying and analyzing traffic on websites, mobile apps, or APIs to identify visits by automated entities instead of humans. In today's digital age, bot detection is an essential security measure, particularly with the growing threat of sophisticated malicious bots that can cause significant damage and widespread fraud. To capture the market, solution providers offer standard firewall protections while incorporating advanced features such as device signals, improving their ability to detect and neutralize malicious bots efficiently.

FIDO2 Authentication

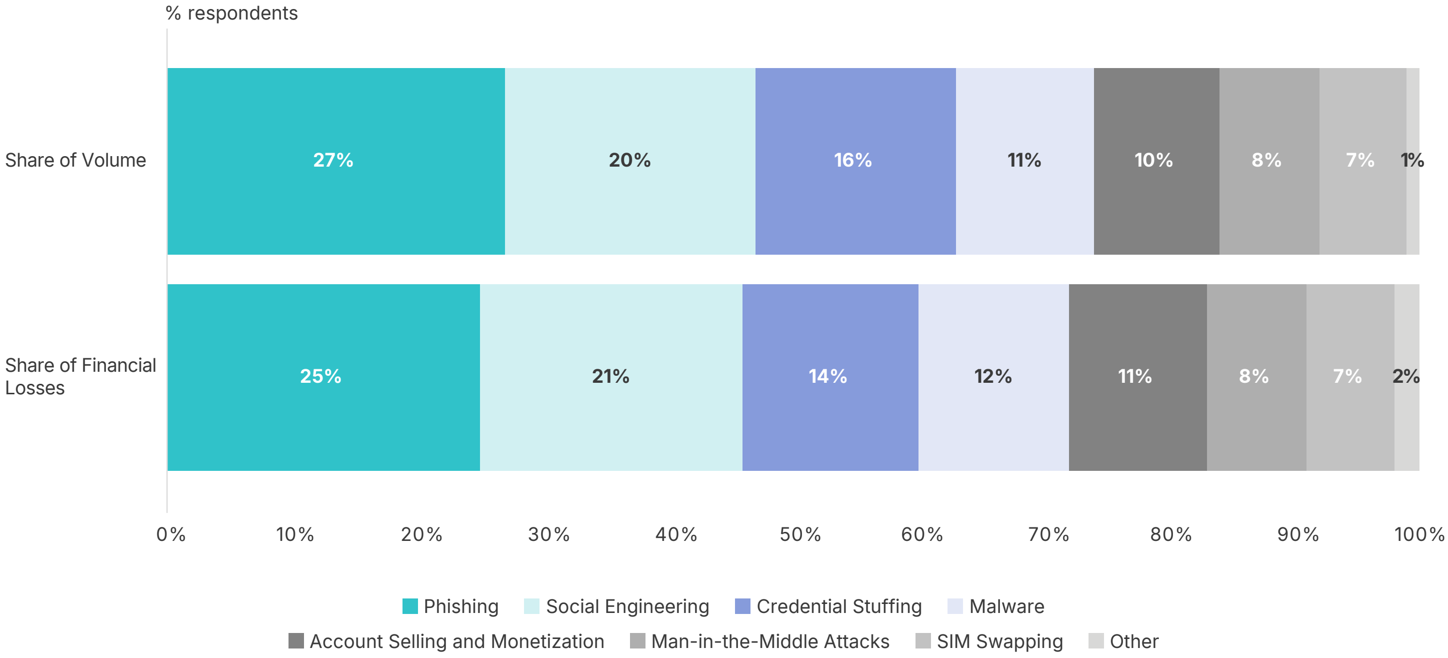
FIDO2 (Fast Identity Online 2) is a set of open standards for authentication that aims to improve the security and convenience of digital authentication. It's a result of a joint effort between the FIDO Alliance and the World Wide Web Consortium (W3C) to create a robust, phishing-resistant protocol for online authentication. FIDO2 allows users to use standard devices such as smartphones, hardware tokens, or biometric readers as authentication methods instead of traditional password-based security. The importance of FIDO2 in preventing account takeover is its ability to significantly reduce dependence on passwords, which are often the weakest link in security. FIDO2 uses cryptographic login credentials that are unique to each website, ensuring that even if data is intercepted, it cannot be reused by an attacker to gain unauthorized access to user accounts on other sites.

Market Dynamics

Market Challenges

Figure 2: ATO Threat Vectors by Volume of Attacks and Share of Financial Losses

Q: 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? (N=50)



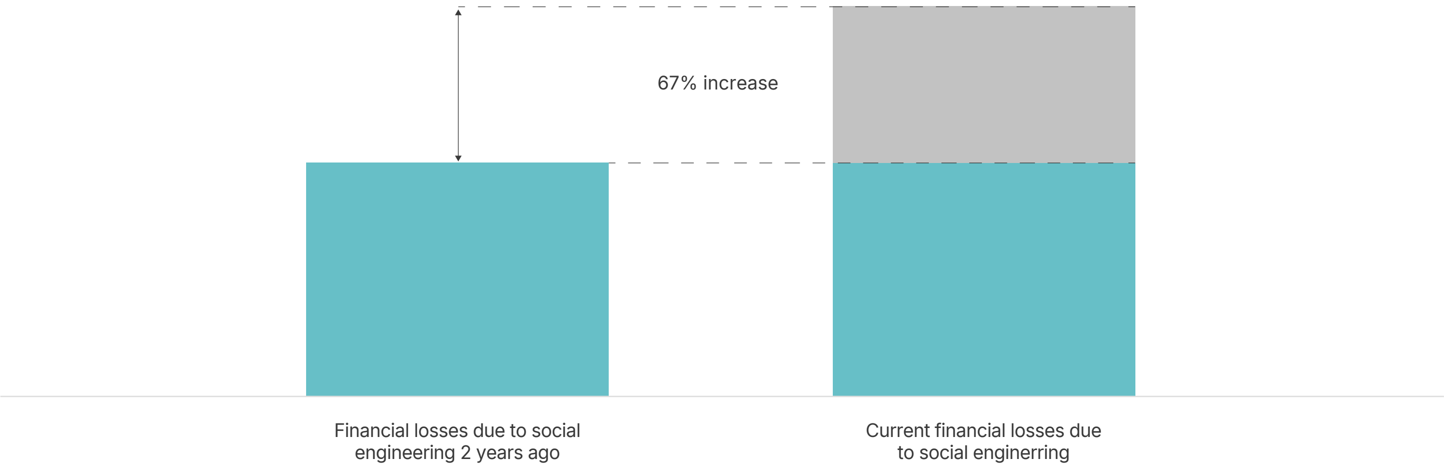
Phishing is the most significant ATO threat vector.

Phishing is the most common way for attackers to access user accounts. This is done by tricking individuals into revealing their login information through deceptive tactics. Phishing attacks can occur through various communication channels, such as emails, text messages, and fake websites. Of the eight principal attack methods, phishing is responsible for 26.7% of all account takeovers, making it the most prevalent threat (see Figure 2).[1]

Bad actors often take advantage of events like tax season and holiday promotions to launch timely phishing attacks that aim to obtain financial data. Financial institutions are particularly at risk, with 25.1% of all financial losses from ATO incidents resulting from phishing attacks (see Figure 2).[1] Phishing attacks require little technical know-how and continue to be an effective means for bad actors to carry out ATO. As such, phishing will likely remain the foremost ATO threat vector in the foreseeable future.

Figure 3: Increase in Financial Losses Due to Social Engineering in the Past 2 Years

Q: Has your organization seen increased or decreased financial losses due to social engineering in the past 2 years? (N=50)



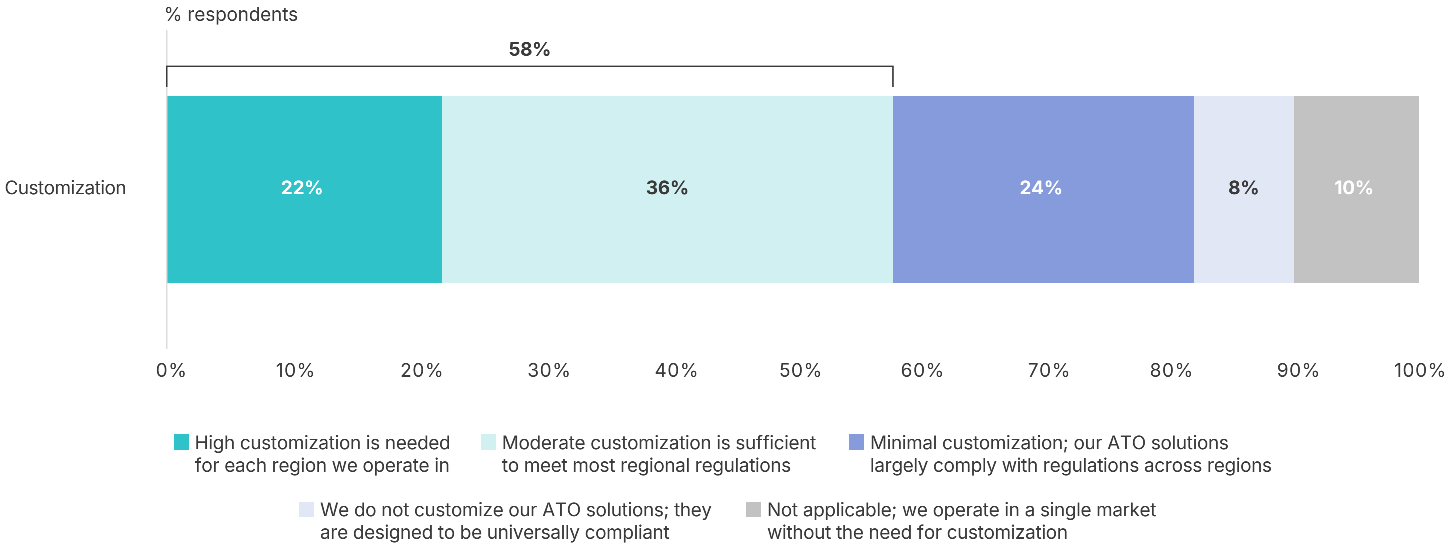
Banks do not effectively address social engineering threats.

Social engineering has emerged as the second most prevalent threat to ATO after phishing. This method exploits human psychology rather than technical flaws to trick people into revealing confidential data. It includes pretexting, baiting, and quid pro quo strategies, where fraudsters fabricate a scenario and offer enticing rewards or benefits in exchange for information.

Social engineering accounts for 20.5% of ATO attack volume and 21.2% of ATO financial losses. Banks have seen a sharp rise of 66.8% in social engineering attacks over the last two years, particularly through social media platforms, enabling fraudsters to gain their victims' trust before exploiting them. This trend has led to increasing demand for comprehensive defenses against social engineering and scams, with 84.0% of banks prioritizing capabilities in detecting such threats, marking it as the second most sought-after ATO protection capability.[1]

Figure 4: Customization Levels Required By Regional Data Privacy Laws

Q: How much customization of your ATO solutions is required to comply with regional regulations? (N=50)



Regional privacy laws require customizable solutions.

Effective prevention of ATO attempts depends on using data signals. However, banks need to balance this requirement with the need to comply with stringent data privacy regulations like the GDPR. These privacy laws restrict the types of personal data organizations can collect, store, and use, thereby limiting banks' access to user behavior data, login patterns, and other signals that can be valuable in detecting ATO attempts.

This has caused concern among financial institutions as most (96.0%) believe that privacy regulations will impede their ability to gather essential data signals for thwarting ATO attempts. Over half of them (54.0%) expect these constraints to materialize within the next two years.[1]

A large majority of banking clients (82%) recognize the need for account takeover (ATO) solutions that are customized to meet diverse regional regulations. Of these, 58% indicate a high to moderate need for such customization, as shown in Figure 4. Additionally, 40% of clients who operate in multiple regions believe it is essential to implement unique solutions for each geographical area.[1]

These insights emphasize the banking industry's struggle to maintain a careful balance between protecting customer privacy and implementing effective measures to prevent account takeover. The industry is concerned that differences in regional laws might require adjustments to their security strategies, and many banks are already adapting to these changes.

Figure 5: Key Vulnerability Points in Login and Account Recovery Processes

Q: Which do you consider to be a bigger vulnerability point, login or account recovery? (N=50)

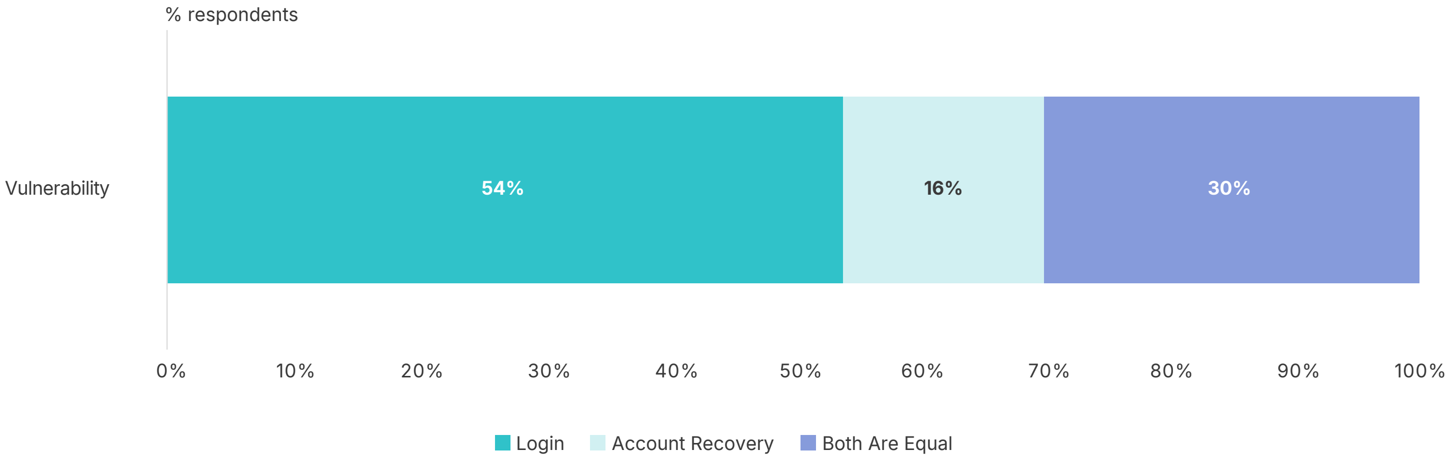
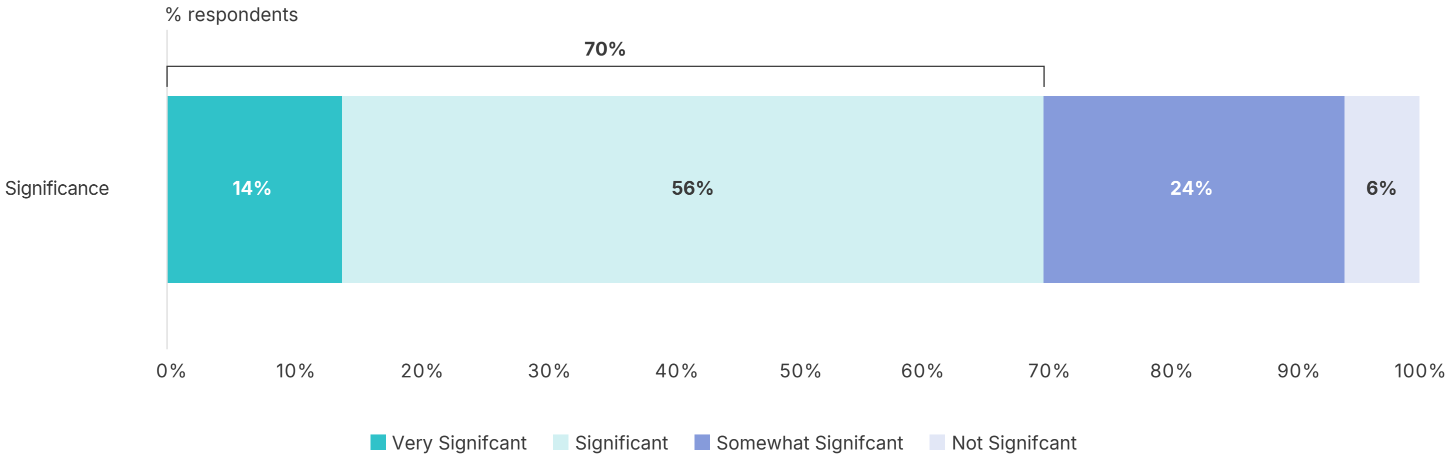


Figure 6: The Significance of Vulnerabilities in Account Recovery Processes

Q: How significant a vulnerability point does your organization consider account recovery? (N=50)



Account recovery remains a vulnerable point as banks prioritize login defense.

The login process of customers is often a point of concern when it comes to ATO threats. This is especially true at banks, where, according to survey respondents, 54.0% consider the login phase a significant vulnerability, as opposed to just 16.0% for account recovery (see Figure 5). However, 94.0% of participants recognize account recovery as a security concern, with 70.0% stating that this concern is very significant or significant (see Figure 6). This suggests that the significance of account recovery might be underestimated, which could lead to an increased risk of security breaches.[1]

The vulnerability of email-based account recovery mechanisms is a major cause of concern because of its widespread use and convenience. A study by the National Science Foundation has shown that 81.1% of website accounts are significantly exposed to threats through email-based account recovery methods.[6] Furthermore, email providers' lack of security improvements exacerbates this issue, which could result in substantial financial and data losses. Therefore, it is essential to re-evaluate account recovery practices to enhance overall security against ATO risks.

Given the significant difference in attention given to login and account recovery procedures, banks should examine their vendor solutions to ensure comprehensive detection across all customer lifecycle stages. While some institutions currently use endpoint ATO solutions that focus primarily on the initial login, switching to platform offerings that cover everything from onboarding and ongoing monitoring to transactions and account recovery would create a more balanced approach to managing risks. Such comprehensive solutions would help banks align their security measures more effectively between login and account recovery stages.

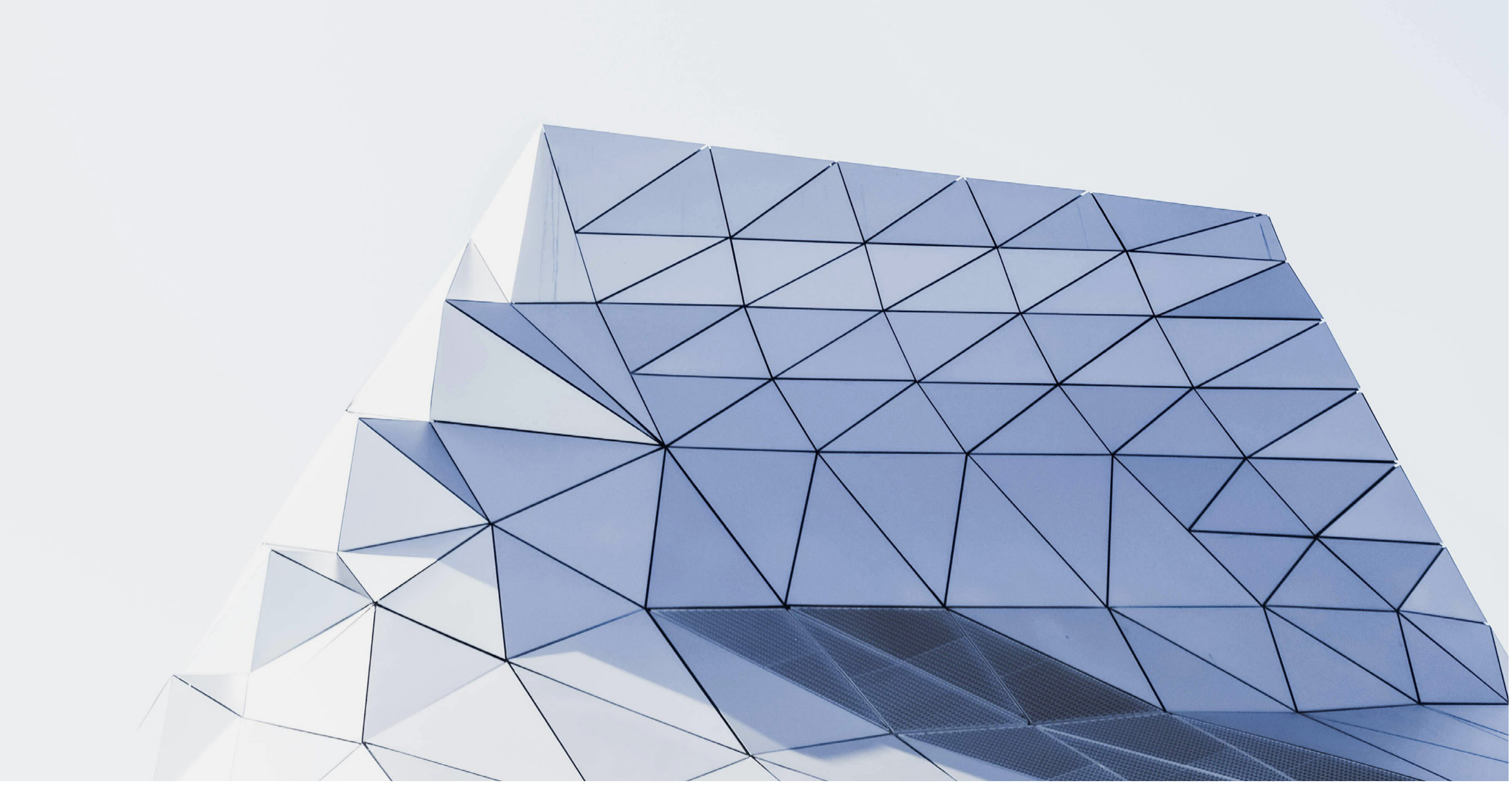
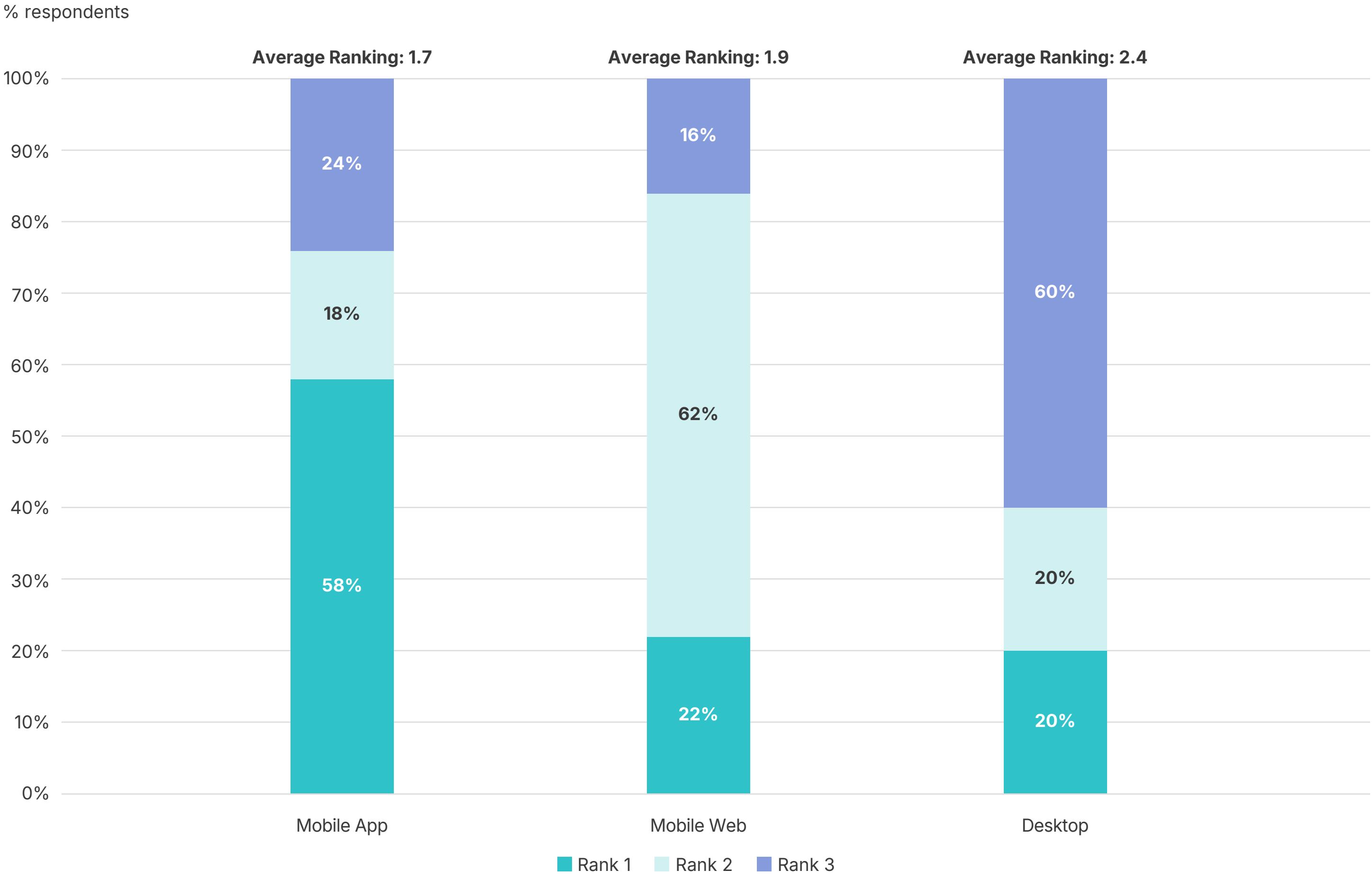


Figure 7: Frequency of ATO Attacks by Mobile App, Mobile Web, and Desktop

Q: Please rank the frequency of ATO attacks on your platform. (N=50)



Most ATO attacks originate from mobile channels, yet few banks utilize mobile device signals.

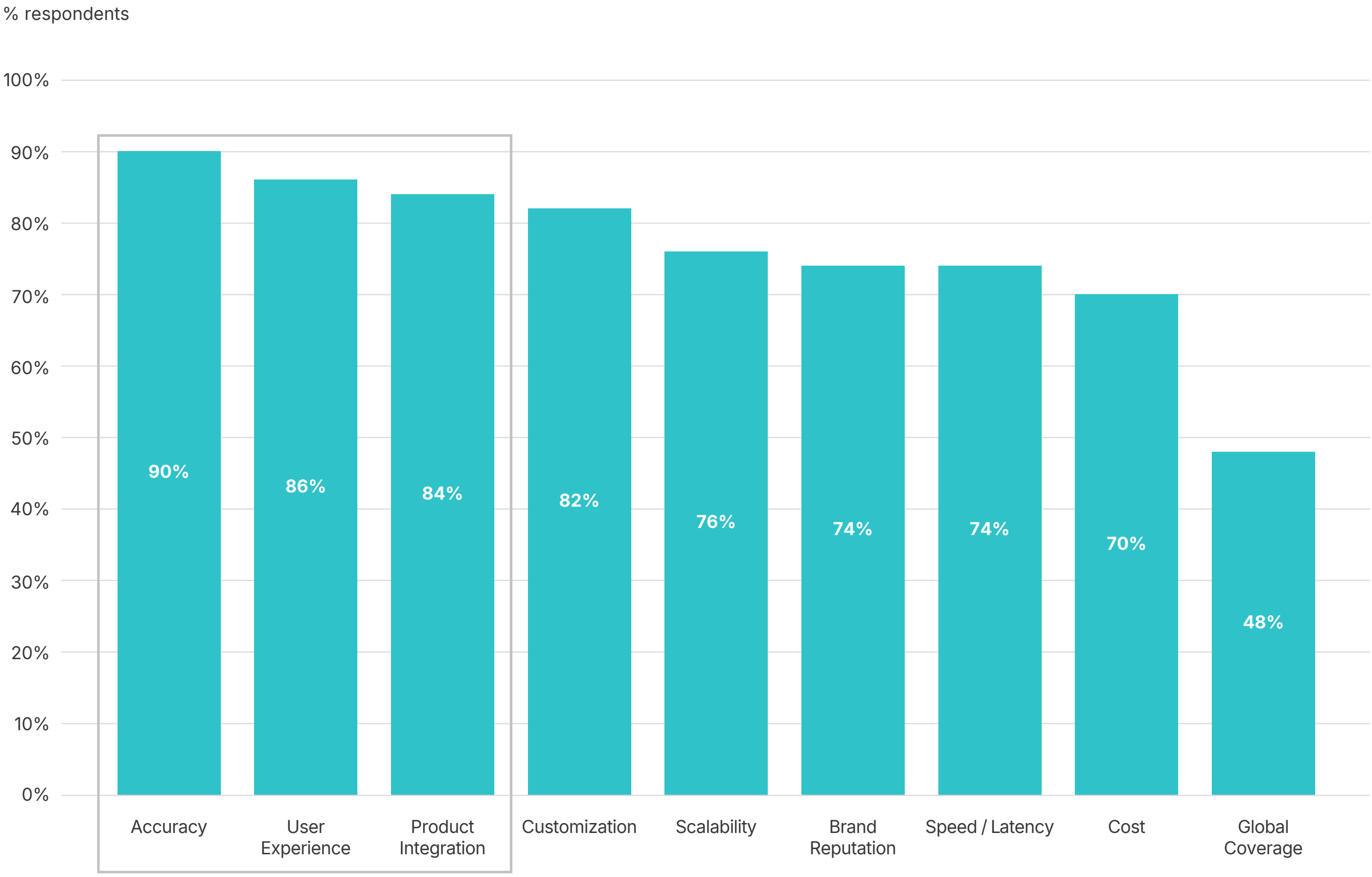
As mobile device usage continues to rise, ATO attacks are shifting towards mobile channels. Banking professionals have ranked mobile apps and mobile web interfaces as the most common avenues for such attacks.[1] The ranking for mobile apps is 1.7 out of 3.0, while for mobile web interfaces, it is 1.9. Desktop channels are less susceptible, with a ranking of 2.4 (as seen in Figure 7). However, despite the clear trend towards mobile vulnerabilities, there seems to be a delay among banks in adopting countermeasures tailored to this evolving threat. Only 44.0% of respondents report using mobile device signals as part of their ATO defense strategies.[1]

The limited adoption of mobile device signals for ATO defense may be due to a focus on other technologies and restrictions on signal access imposed by device manufacturers. This neglect of mobile device signals poses a significant risk to the banking industry, especially as mobile channels become increasingly prevalent. As reliance on mobile apps and web interfaces grows, a corresponding increase in ATO attacks can be expected. SMS OTP, used by 80.0% of survey respondents and the second most popular authentication method, becomes particularly risky without the support of mobile device signals.[1] Without these signals, vulnerabilities like SIM swapping, where a fraudster transfers a victim's phone number to a new SIM card they control, remain a serious threat. This highlights the critical need for enhanced mobile security measures.[7]

Market Demands

Figure 8: Key Purchasing Criteria (KPC) for ATO Prevention in Banking

Q: How would you prioritize the key purchasing criteria for ATO solutions? Rate from least 1 (least important) to 5 (most important). *"Highly demanded" refers to choices rated as 4 or 5 on a scale from 1 to 5, where 1 signifies least important and 5 denotes most important. (N=50)



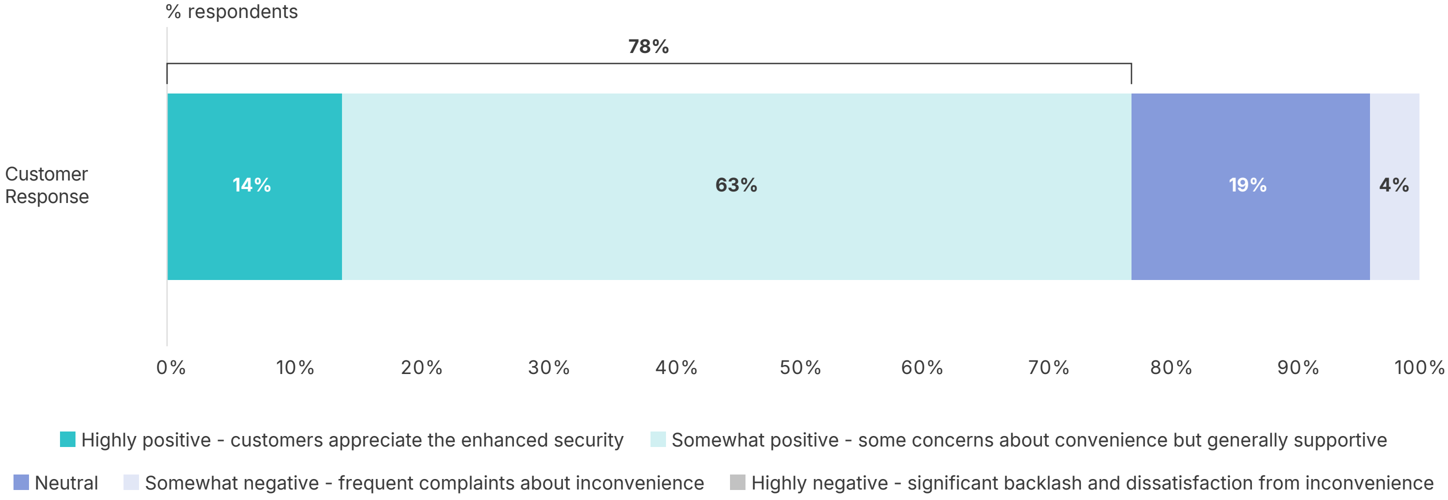
Banks view accuracy, user experience, and product integration as top Key Purchasing Criteria (KPC).

Banking executives prioritize accuracy (90.0%), user experience (86.0%), and ease of product integration (84.0%) when selecting solutions ATO (see Figure 8). This is because successful ATO incidents can result in significant financial losses, requiring a combination of signals and authentication techniques. A seamless user experience that keeps customers happy is equally important, with banks seeking providers who can balance the right amount of security measures to maintain high customer satisfaction while minimizing fraud. Additionally, banks prefer solutions that can be integrated easily and quickly without requiring much time or resources for implementation.[1]

To deliver highly accurate ATO solutions while ensuring a positive user experience, providers can utilize product capabilities that rely on passive signals such as behavioral analytics, behavioral biometrics, and continuous authentication. These technologies minimize user friction by leveraging indicators of risky behavior, such as unusual mouse movements or typing patterns, without disrupting the user experience. Notable vendors often provide API or low-code/no-code solutions, enabling banks to implement these technologies swiftly and streamline their operational setup.

Figure 9: Customer Response to Heightened Security Measures

Q: How have customers responded to increased security measures that require more user interaction? (N=50)



Banks understand the importance of providing secure services to their customers.

Financial institutions, particularly banks, use multi-factor authentication (MFA) to safeguard user accounts from unauthorized access. This process involves multiple layers of authentication for customers to access their accounts. A vast majority of banks (98%) have implemented various authentication methods to bolster security. Unlike other sectors where complex security measures may dissuade users, bank customers generally welcome these precautions. This acceptance stems from the reassurance that additional security provides about the safety of their accounts. According to banking executives, 77.6% of customers have reacted positively to these enhanced security measures, despite some associated inconvenience (refer to Figure 9). However, it's crucial to balance these security measures with user experience, which 86% of banking decision-makers consider extremely important, making it a primary concern right after security.[1]

Figure 10: Product Capabilities Demand for ATO Prevention in Banking

Q: How would you prioritize the following product capabilities when evaluating ATO solutions? Rate from least 1 (least important) to 5 (most important). Note: "Highly demanded" refers to choices rated as 4 or 5 on a scale from 1 to 5, where 1 signifies least important and 5 denotes most important. (N=50)

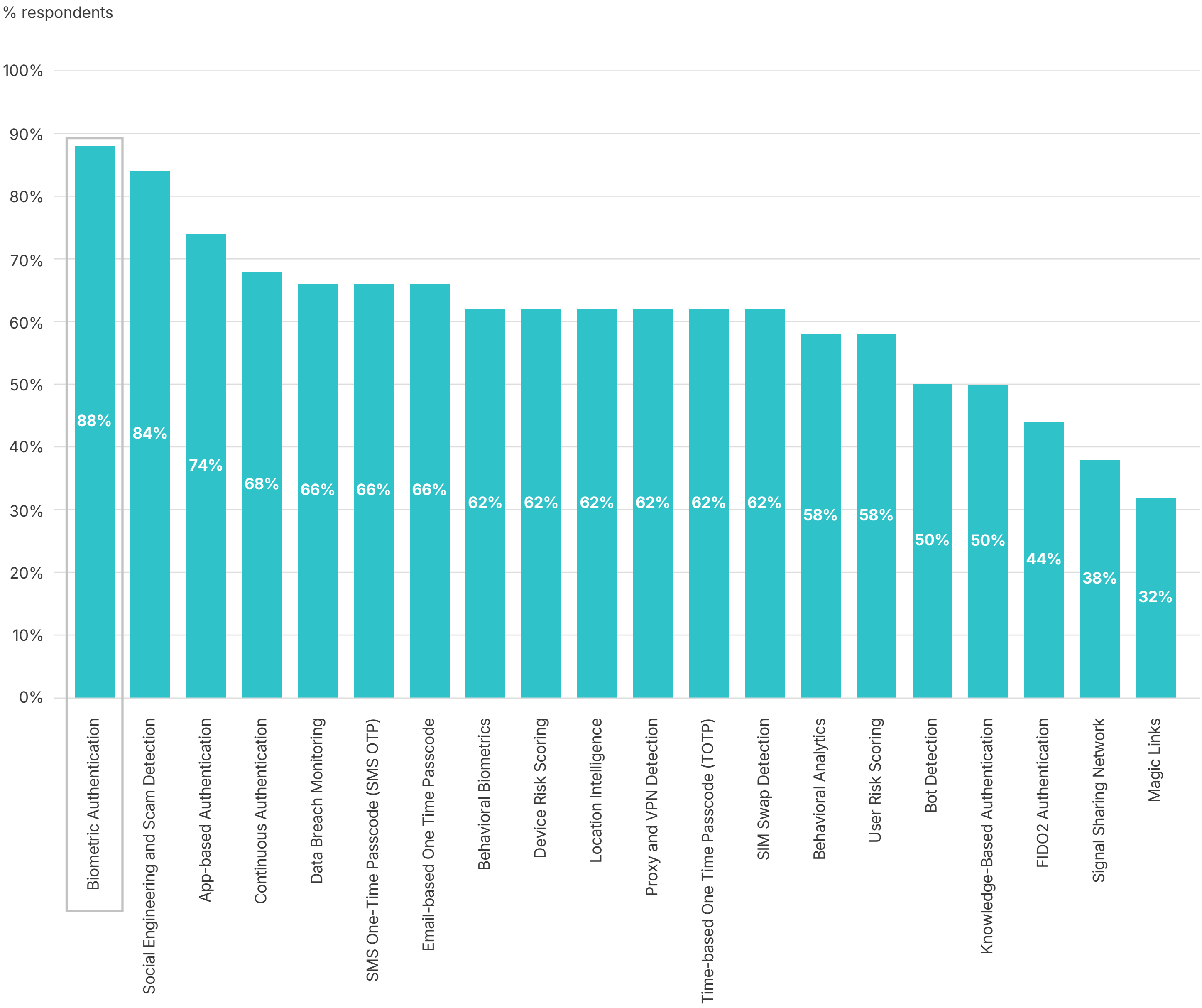
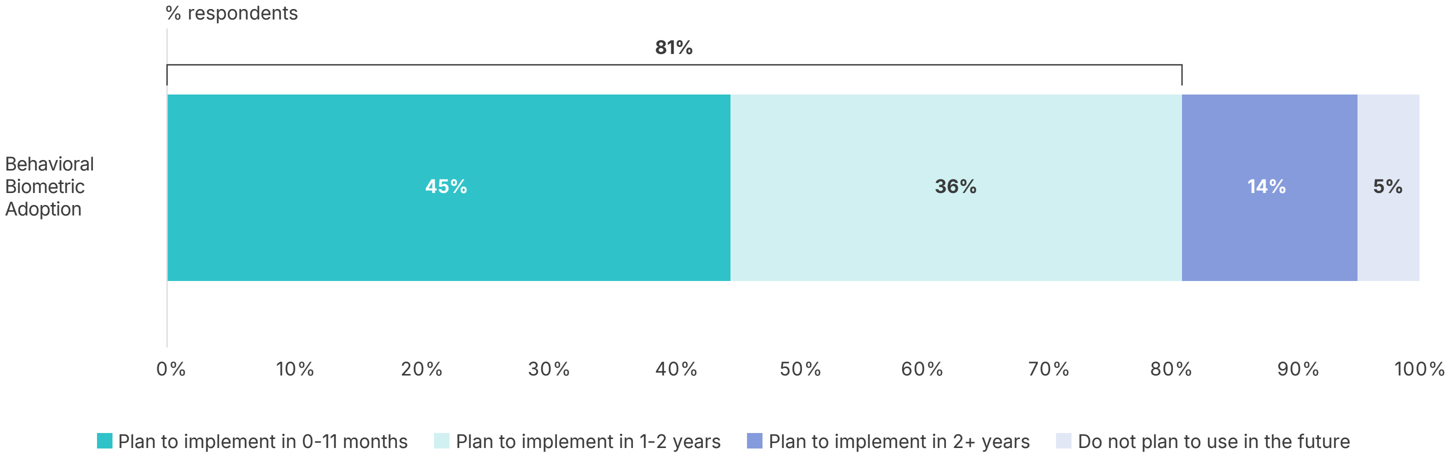


Figure 11: Plans for Behavioral Biometric Adoption Among Current Non-Adopters

Q: You previously mentioned that you are not currently leveraging behavioral biometrics for ATO prevention. Please describe your company's future desire to leverage this type of solution. (N=22)



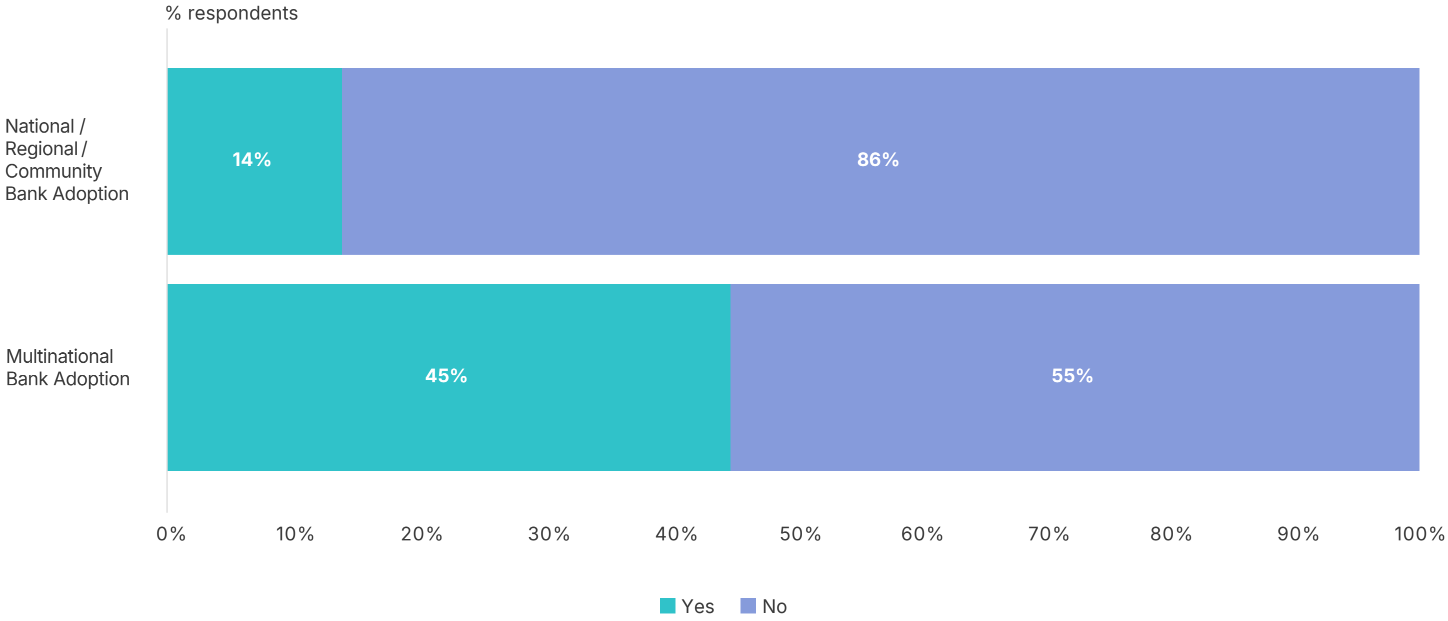
Biometric solutions are becoming increasingly popular for preventing ATO at banks.

Authentication methods generally fall into three categories: knowledge-based (like passwords or personal information), possession-based (such as cryptographic devices or tokens), and inherence-based (biometric identifiers). However, knowledge-based authentication is not highly demanded for ATO prevention, ranking 17th among 20 capabilities. Meanwhile, tokens are not yet widely accepted as authentication. On the other hand, biometric methods are gaining popularity as they are considered more user-friendly than token-based approaches, which can create friction in the authentication process. An overwhelming 88.0% of survey participants strongly prefer biometric authentication, making it a highly demanded capability for combating account takeovers (see Figure 10).[1]

Banks are also turning to behavioral biometrics as a sophisticated approach to ATO prevention. This technique analyzes the unique patterns in an individual’s behavior, such as typing cadence, mouse movements, and interaction with touchscreens, to verify identity. Combining these behavioral signals creates a user's distinct profile over multiple sessions, serving as a reference point for future authentications. Currently, 56.0% of survey respondents utilize behavioral biometrics. Of those who have not adopted it yet, 81.8% plan to implement it within the next two years (see Figure 11), indicating its growing significance in the banking industry’s security strategies.[1]

Figure 12: Continuous Authentication Adoption By Bank Type

Q: What types of authentication modalities are you leveraging for account takeover protection? Note: Responses below are for Continuous Authentication adoption. (N=50)



Banks of different sizes adopt specific product capabilities differently, with the most significant difference observed in adopting continuous authentication.

Large multinational banks are over three times more likely to use continuous authentication than national, regional, and community banks (see Figure 12). Continuous authentication is a security method that continuously verifies a user's identity throughout their session, not just at login. It provides a more secure and seamless approach by responding to potential threats in real time.

Despite this disparity in usage, the interest in continuous authentication is almost equal across all bank sizes, with 69.0% of multinational banks and 66.7% of smaller banks expressing high demand for the capability. However, continuous authentication is typically more expensive than other popular solutions, such as various OTP methods, often costing about 20.0% - 40.0% more. This may explain its less frequent use among smaller institutions. While the desire for advanced ATO prevention solutions is universal, multinational banks have greater resources to invest in and implement these sophisticated security measures.[1]

Market Opportunities and Drivers

The increasing sophistication and frequency of attacks have heightened the demand for ATO prevention solutions for banks. Financial institutions are acutely aware of the substantial losses they face from successful ATO attacks, with our buyer survey indicating an average fraud loss of $6,232 per incident.[1] This exposure prompts banks to continuously reassess their fraud prevention strategies, often seeking additional solutions. Vendors can engage this market by offering advanced technologies and effective fraud prevention methods, aligning their products with the evolving needs of banking organizations for robust ATO protection.

Methodology

To assess the size of the account takeover prevention market across banks, we segmented the market size by the size of the banks. We did this as the purchasing methods and pricing for ATO solutions vary depending on the size of the bank. We specifically differentiated banks based on their asset size:

- **SMB/Community Banking Institutions:** Less than $10.0 billion in assets
- **Regional Banking Institutions:** $10.0 billion to $100.0 billion in assets
- **National Banking Institutions:** $100.0 billion to $500.0 billion in assets
- **Multi-National Banking Institutions:** $500.0 billion or more

Quantity

Our analysis began by examining third-party data from the FDIC and SNL Financial to determine customer account numbers by different-sized banking organizations. We categorized financial institutions by their asset size (see designations above) to better discern ATO prevention trends across various scales of banks, ranging from smaller community banks to large, enterprise-level institutions. We determined that the percentage of total bank accounts by size of banking organizations is as follows:

- **SMB/Community Banking Institutions:** 30.4% of all total customer accounts
- **Regional Banking Institutions:** 31.4% of all total customer accounts
- **National Banking Institutions:** 19.6% of all total customer accounts
- **Multi-National Banking Institutions:** 18.6% of all total customer accounts

Quantity Driver: Digital Banking Penetration Increase

The market for ATO prevention solutions is on track for expansion, fueled by the growing commitment of financial institutions to enhance their digital banking solutions. Consumers globally are increasingly adopting digital methods, including in the realm of banking. Digital banking simplifies and streamlines processes such as withdrawing money, transferring funds, paying bills, opening accounts, and managing finances. The penetration of digital banking in North America, Europe, Middle East, Africa, and Asia Pacific is expanding, with a CAGR of approximately 3.0 - 5.0%. Meanwhile, in Latin America, the growth is even more rapid, with a CAGR exceeding 6.0%.

This surge in digital banking is expected to contribute approximately 5.0% to the total CAGR throughout the forecast period.[2] According to the World Bank, in 2024, 27.1% of the global population engaged in banking via digital platforms, though exact levels vary by country/region.[8] We used historical data on digital banking penetration rates, including mobile and web banking adoption rates, to predict the increase in digital banking penetration by region. The anticipated annual digital banking penetration growth rates for various regions during the forecast period are as follows:

- **North America:** 3.3% CAGR in digital banking penetration over the forecast period
- **Europe, Middle East, and Africa:** 4.2% CAGR in digital banking penetration over the forecast period
- **Asia Pacific:** 4.3% CAGR in digital banking penetration over the forecast period
- **Latin America:** 6.6% CAGR in digital banking penetration over the forecast period

Pricing

We found that pricing is highly scale-dependent, with larger banks securing substantial per-user discounts. Vendors implement tiered pricing strategies, offering lower rates per user as the size of the user base increases. This approach allows vendors to attract larger clients by aligning cost savings with customer scale. Using pricing data from our buyer survey and publicly available vendor information, we established an annual per-user cost ranging from $0.20 to $1.86 for account takeover prevention solutions, which varies based on user volumes and the extent of product features utilized.

Pricing Driver: Pricing Increase Expectations

Additionally, we expect the pricing of ATO solutions to rise throughout the forecast period. On average, banking buyers anticipate an annual price increase of 6.5% for these solutions, driven by ongoing trends in pricing and the shift towards more advanced technologies.[1] This expected rise in costs reflects inflationary pressures and a heightened demand for more sophisticated ATO solutions as key threats, like phishing and social engineering, become increasingly prevalent and complex.

Account Takeover Prevention in Banking Market Size

Considering the factors of growing digital banking penetration and the evolving pricing structures for ATO prevention solutions, we project the global total addressable market (TAM) for these solutions for banks to be approximately $954.8 million in 2024. The market is expected to expand to $1.5 billion by 2028, demonstrating a CAGR of 9.3% during the forecast period.[2]

Figure 13: Account Takeover Prevention in Banking Solution Market Size (2024-2028)

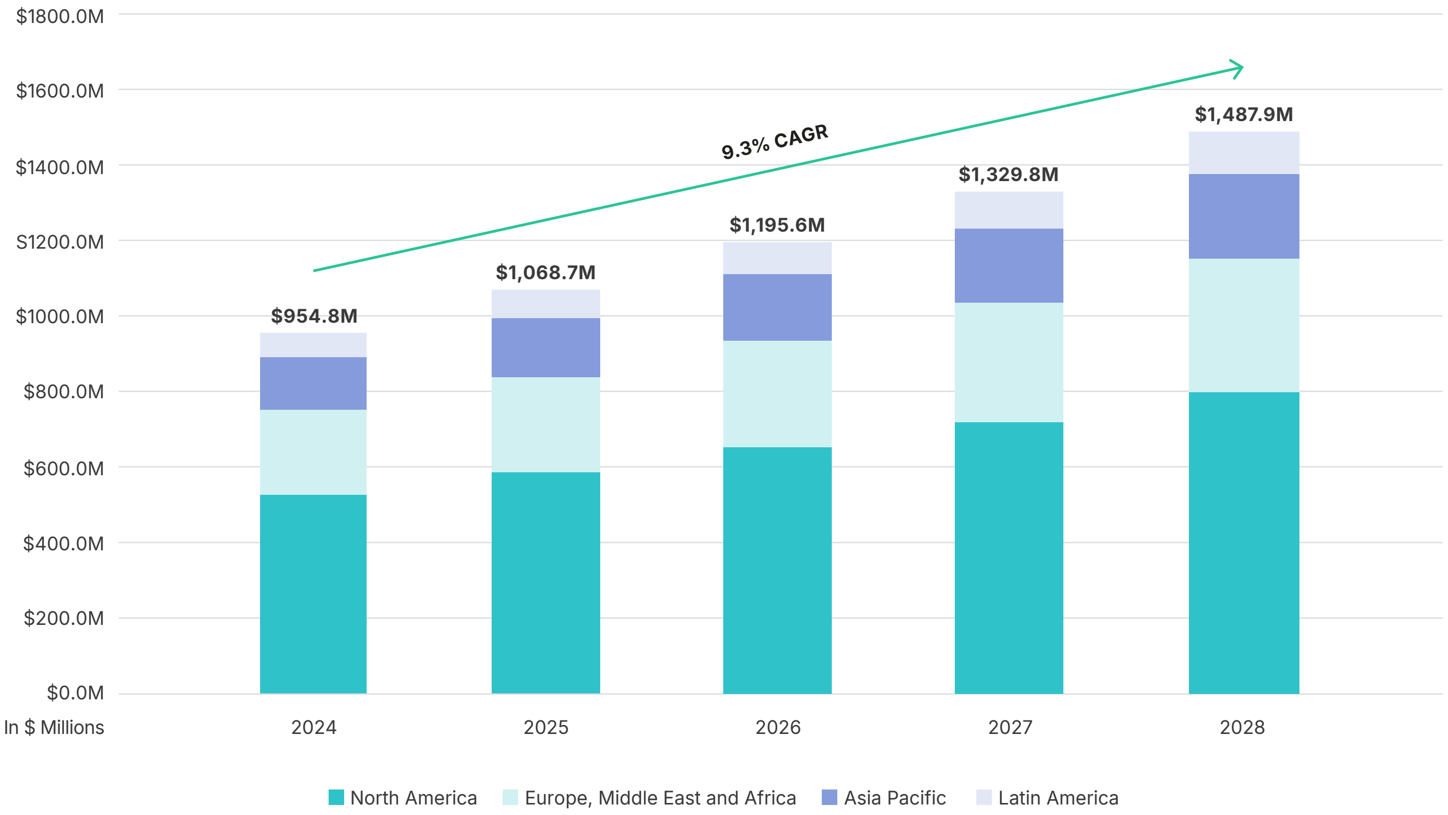


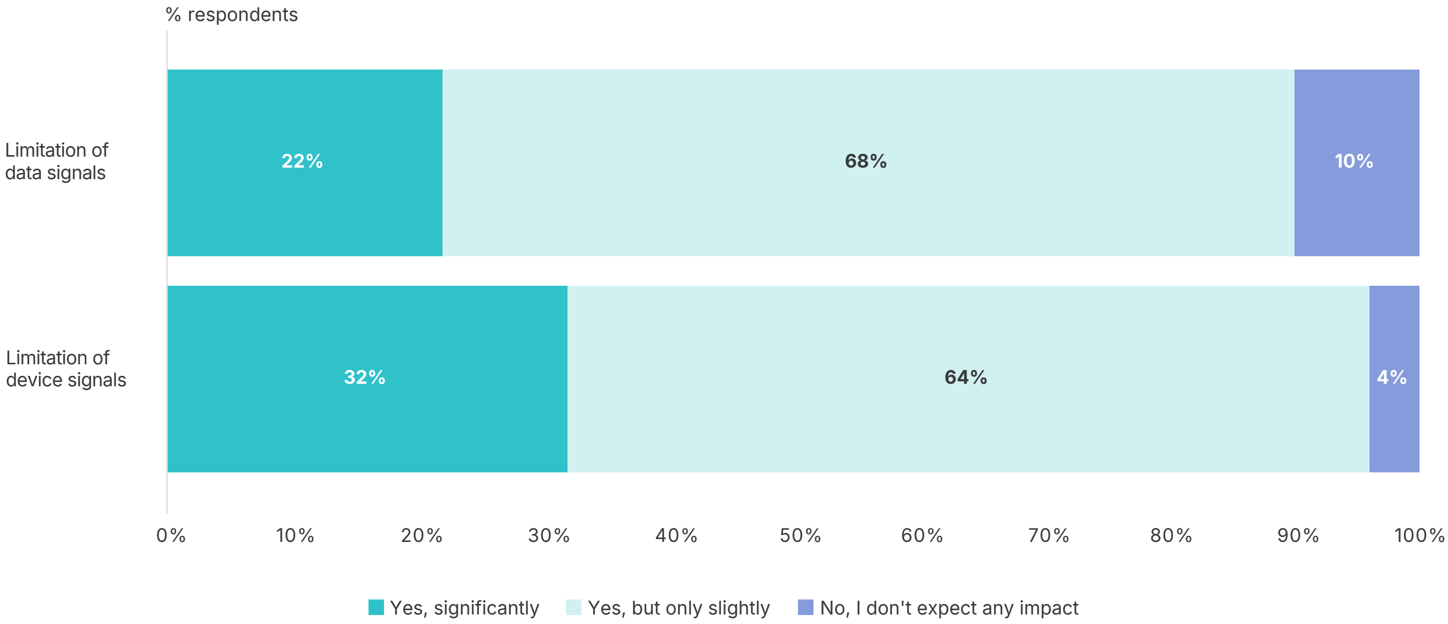
Table 2: Account Takeover Prevention in Banking Solution TAM by Banking Customer Size (2024-2028)

(USD Millions)	2024	2025	2026	2027	2028	CAGR
North America	527.2	586.4	652.9	719.6	799.1	8.7%
Europe, Middle East and Africa	224.2	251.6	282.4	315.9	354.7	9.6%
Asia Pacific	139.5	156.6	175.3	196.7	221.2	9.7%
Latin America	63.8	74.1	85.0	97.6	112.8	12.1%
Total	**954.8**	**1068.7**	**1195.6**	**1329.8**	**1487.9**	**9.3%**

Future Outlook

Figure 14: Significance of Limitation of Signals from Big Tech

Q: Do you expect the limitation of device signals from manufacturers (such as Apple) to reduce your organization's ability to prevent ATO? AND Do you expect the limitation of digital signals from tech companies (such as Chrome cookies) to reduce your organization's ability to prevent ATO? (N=50)

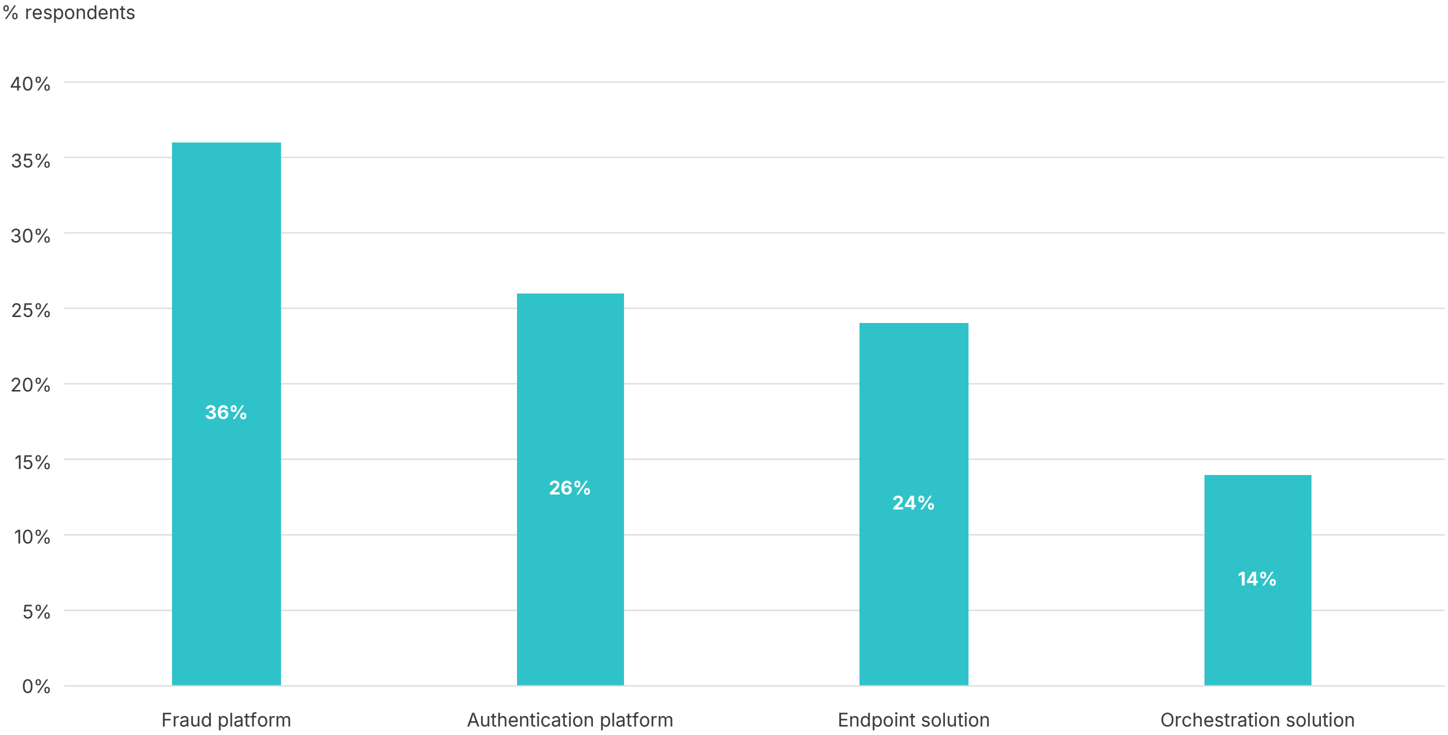


Banks expect Big Tech data restrictions to make their ATO solutions less effective.

Banks are worried that restrictions on data signals by major technology companies such as Apple and Google could have a negative impact on their ability to prevent ATO attacks. According to our survey, 96.0% of banking professionals believe that limiting access to device signals could undermine their ATO solutions, while 90.0% have similar concerns about other types of data signals, like Chrome cookies.[1] These concerns highlight the significant influence that major technology companies hold over security practices and the potential challenges that banks and ATO solution providers may face in dealing with ATO prevention. For example, Apple's recent privacy features that allow users to control app tracking and data sharing and Google Chrome's plan to phase out cookies by 2024 could impact security measures.[9, 10] Therefore, banks and ATO solution providers must remain vigilant in tracking how policy changes by major tech firms could affect their security measures.

Figure 15: Preference Between Fraud Platforms, Authentication Platforms, Endpoint Solutions, and Orchestration Solutions for ATO Prevention

Q: What do you value most in an ATO solution? (N=50)

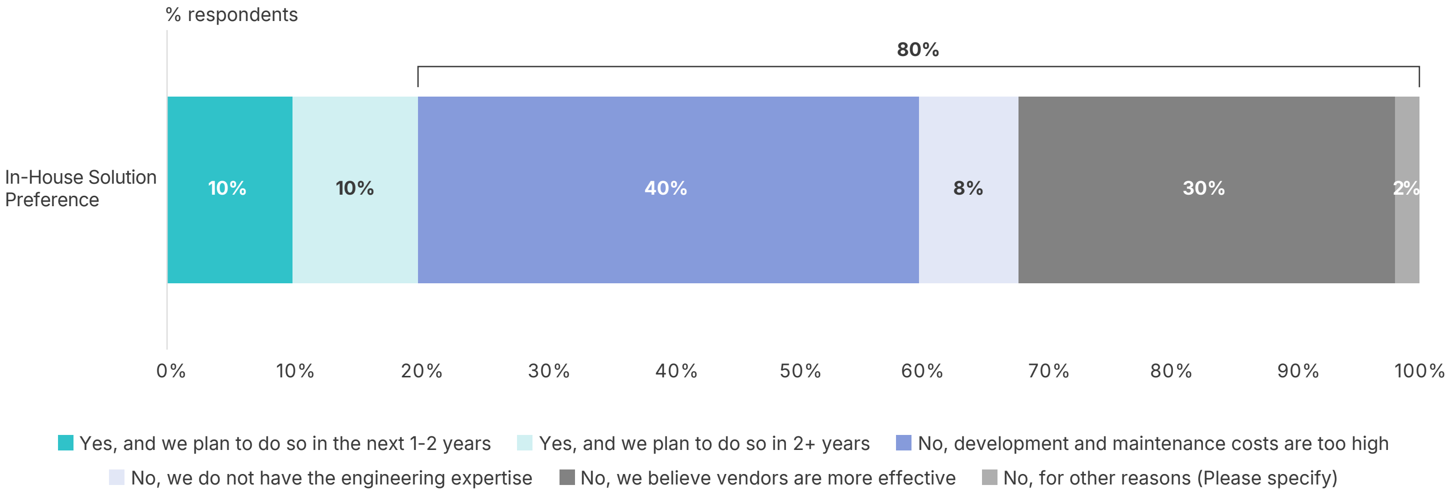


Fraud and authentication platforms will compete with endpoint solutions for banking customers.

The competition among vendors in the banking industry is expected to intensify, with fraud and authentication platforms competing with endpoint solutions. While both authentication and fraud prevention and detection vendors address ATO, they do so through different approaches. Authentication providers establish barriers to deter malicious entities, whereas fraud prevention systems rely on analyzing behavioral signals to identify and respond to unusual activities. Furthermore, their product offerings differ, with authentication solutions often including broader access management features and fraud prevention tools extending beyond ATO safeguards to areas such as chargeback management. In contrast, endpoint providers focus specifically on ATO and have limited additional use case coverage. Our survey revealed varied preferences, with 36.0% of respondents favoring fraud prevention platforms, 26.0% leaning towards authentication services, and 24.0% opting for top-tier endpoint solutions (see Figure 15).[1] This diversity of choice contrasts with the recent trend towards Integrated Identity Platforms, which offer comprehensive coverage across the entire customer journey and are preferred by two-thirds of identity solution purchasers.[11]

Figure 16: Preference for In-House ATO Solutions and Reasons for Using Vendors

Q: Has your organization considered bringing your ATO solution entirely in-house? (N=50)



Banks will continue to turn to vendors for ATO prevention and will not bring solutions in-house.

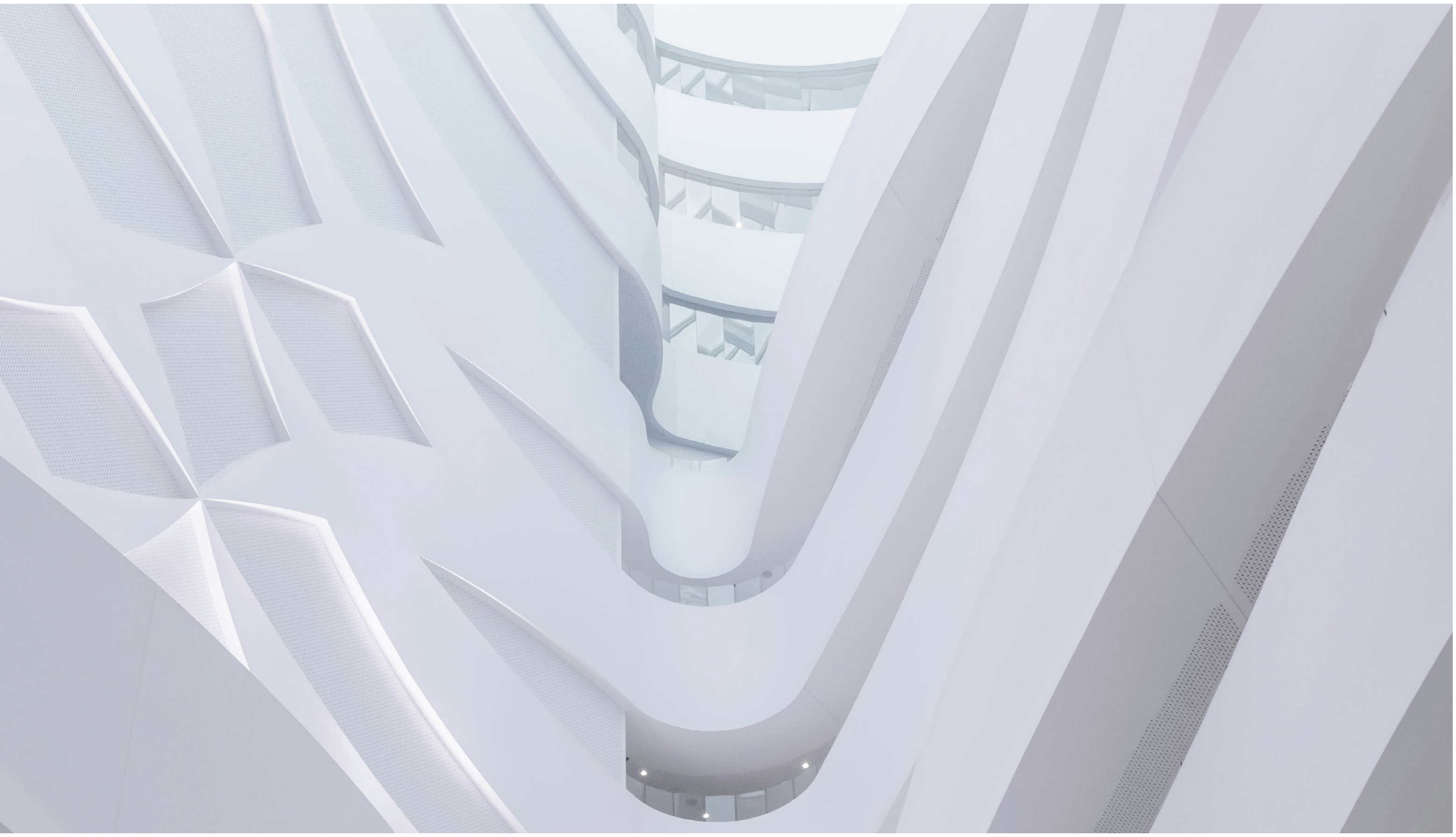
Banks are unlikely to develop their own ATO prevention solutions due to the complexity of such solutions, which employ diverse methods and provide extensive coverage of threat vectors. As a result, banks will continue to rely on external vendor solutions. Only 20.0% of fraud teams have reported plans to develop ATO solutions in-house, with half not expecting to do so for at least two years (see Figure 16).[1] High costs of development and maintenance, as well as perceived inferior effectiveness compared to external vendor solutions, are the primary deterrents. Interestingly, larger and smaller institutions share the same inclination towards in-house development, with 20.7% of multinational banks considering full in-house implementation, closely mirrored by 19.0% of national, regional, and community banks.[1]

Conclusion

Our study of the ATO prevention market within the banking industry provides pivotal insights and trends currently shaping this field. This research is particularly valuable for banking executives grappling with significant fraud losses due to account takeovers. The industry faces significant hurdles, notably phishing attacks, the most common cause of ATO incidents and financial losses. Additionally, social engineering has emerged as a significant and growing threat. Banks must also navigate upcoming constraints on data usage imposed by Big Tech firms like Apple and Google, alongside evolving regional privacy regulations. This complex environment necessitates flexible, region-specific ATO solutions that adhere to legal standards without compromising fraud prevention efficacy.

Despite these obstacles, the demand for ATO prevention solutions is rising. Financial institutions are keenly aware of the financial implications of ATO incidents and are actively seeking effective strategies to mitigate these risks and maintain trust in their digital platforms. More banks increasingly rely on biometric authentication and exploring behavioral biometrics, which utilize passive signals for enhanced threat detection, balancing sophisticated security with user experience.

In summary, banks are tasked with bolstering their current security measures and staying ahead of technological and regulatory shifts. Successfully integrating advanced security technologies with customer experience and compliance is essential for sustaining the security and integrity of banking platforms amidst these evolving challenges.



Notable Solution Providers

Below is an overview of the notable vendors in the ATO solutions space, which includes providers specializing in authentication and fraud prevention and others offering more specifically tailored endpoint solutions, each offering a unique array of product capabilities. Banks should carefully assess their own needs against the capabilities of these vendors, taking into account both currently in-demand features and those expected to rise in importance. By aligning their resources with the right vendor features, banks can effectively mitigate the increasing threats of account takeovers now and in the future.

Table 3: Notable ATO Prevention Solution Providers in Banking

Vendor		
1Kosmos	Experian	Nethone
Accertify	Feedzai	Nevis Security
Akamai Technologies	Fortinet	OneSpan
Alessa	GBG	Outseer
Anonybit	GeoComply	Palo Alto Networks
Appgate	HUMAN	Ping Identity
Arkose Labs	Imperva	Prove
BioCatch	IBM (Trusteer)	SecureAuth
Bureau	Incognia	SHIELD
Caf	Instnt	Socure
Callsign	iProov	SpyCloud
Cybersource	Jumio	Telesign
DataDome	Keyless	TMT ID
DataVisor	Kount	Transmit Security
Deep Labs	LexisNexis Risk Solutions	TransUnion
Duo Security	Mastercard (NuData)	Uniken
Entersekt	Netcraft	Veridium
Entrust	NeuroID	ZeroFox

Appendix

Definition of Terms

Table 4: Important Terms Mentioned in This Report

Term	Definition
Account Selling and Monetization	After gaining access to an account, attackers may use it for their gain (e.g., transferring money, making purchases) or sell the account credentials on the dark web. This is particularly common with accounts storing financial information or other valuable data.
App-based Authentication	App-based authentication, such as the use of an authenticator app, is a method that provides an additional layer of security for online accounts through multi-factor authentication (MFA). These apps generate time-based, one-time passcodes (TOTP or OTP) on a user's smartphone, which must be entered in addition to the usual login credentials (like a password) to access an account.
Behavioral 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.
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.
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. Biometric authentication can use physical biometrics (based on physiological features) and behavioral biometrics (based on how people behave).
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.
Continuous Authentication	Continuous authentication is a security approach that verifies a user's identity throughout a session rather than just at the login point.
Credential Stuffing	Credential Stuffing involves attackers using stolen usernames and password pairs to gain unauthorized access to accounts across multiple platforms. This method relies on many users reusing their login credentials across different services.

Term	Definition
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.
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.
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.
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.
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?")
Location Intelligence	Location intelligence leverages geolocation data to understand user behavior, deliver personalized services, and enhance marketing strategies based on real-time location information.
Magic Links	Magic links are a one-time use link sent to the customer during the authentication process, enabling passwordless authentication.
Malware	Malware, including Trojans and spyware, can capture login credentials directly from users' devices. Once installed, malware can record keystrokes or manipulate legitimate banking apps to steal sensitive information.
Man-in-the-Middle (MitM) Attacks	MitM attacks involve intercepting the communication between two parties without their knowledge. Attackers can use this method to capture login credentials or other sensitive information transmitted over unsecured or compromised networks.
Phishing	Phishing scams trick users into providing their login credentials by masquerading as trustworthy entities. Attackers use various forms of communication, including emails, text messages, and fake websites, to deceive victims.
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).
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.

Term	Definition
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.
SIM Swapping	SIM swapping is a technique where the attacker convinces a mobile carrier to switch the victim’s phone number to a SIM card controlled by the attacker. This allows them to intercept two-factor authentication (2FA) codes and gain access to secured accounts.
SMS 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.
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.
Social Engineering	Social engineering attacks manipulate individuals into divulging sensitive information. These attacks exploit human psychology rather than technical vulnerabilities and can take various forms, including pretexting, baiting, and quid pro quo schemes.
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.
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.

Survey Demographics

Figure 17: Respondents by Business Unit

Q: Which business unit are you most closely associated with? (N=50)

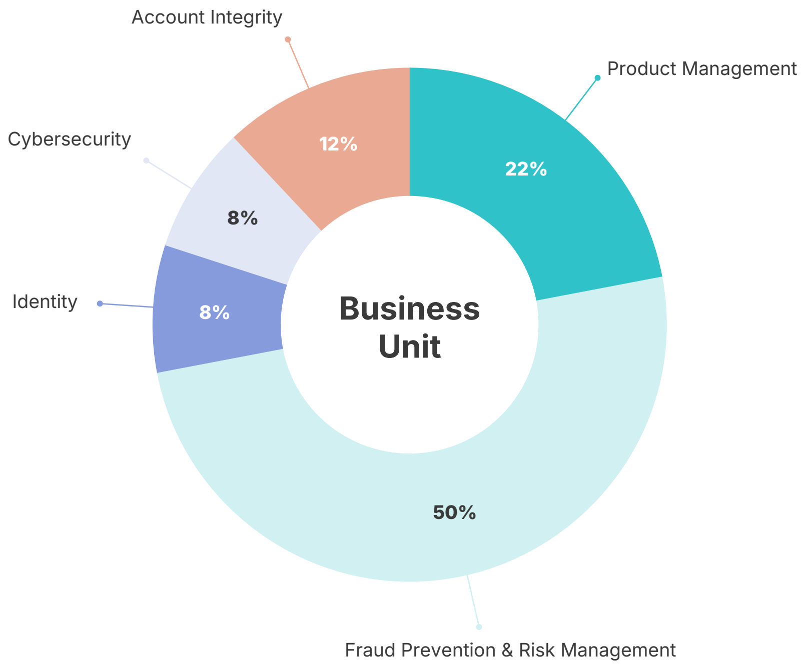


Figure 18: Respondents by Self-Reported Job Level

Q: What level most closely aligns with your job level? (N=50)

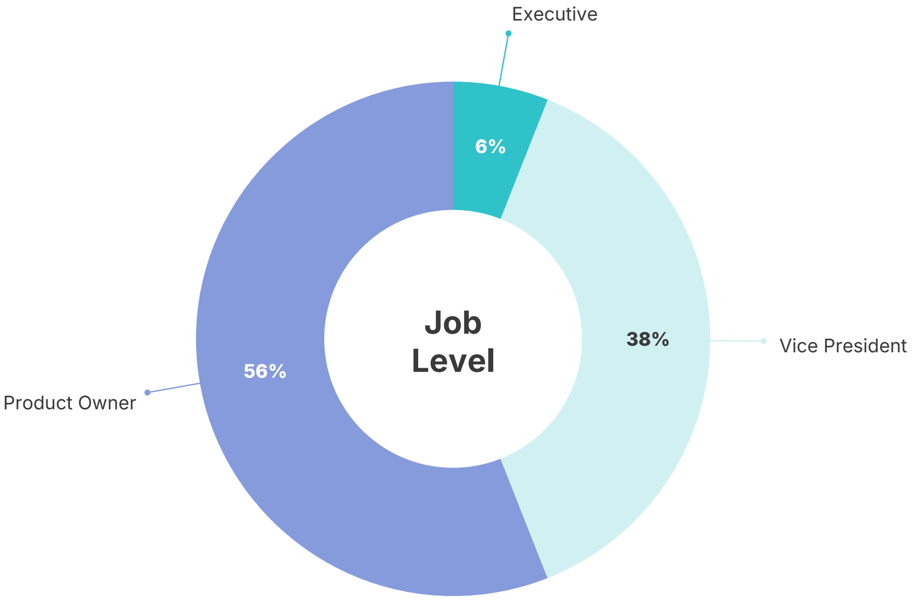


Figure 19: Respondents Geographic Coverage

Q: What is your company’s geographic coverage? (N=50)

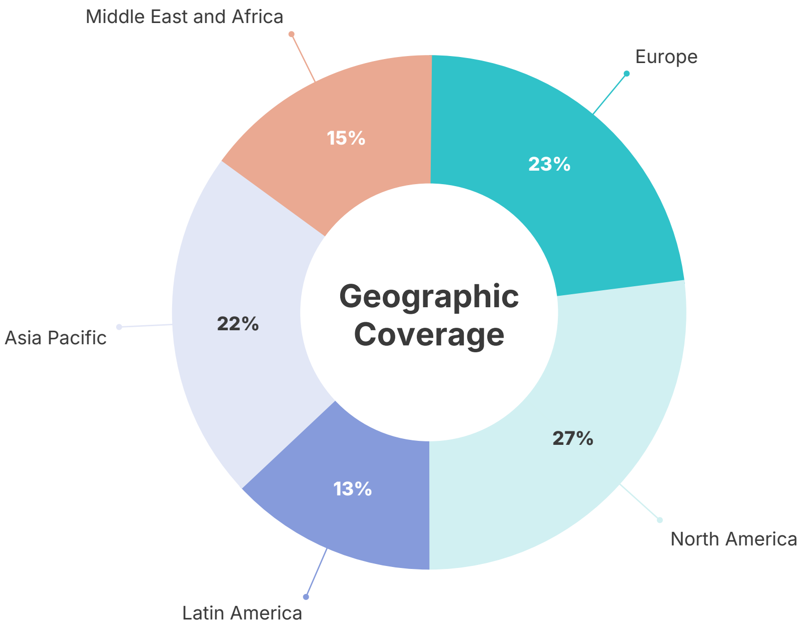


Figure 20: Respondents User Count

Q: How many users does your organization have? (N=50)

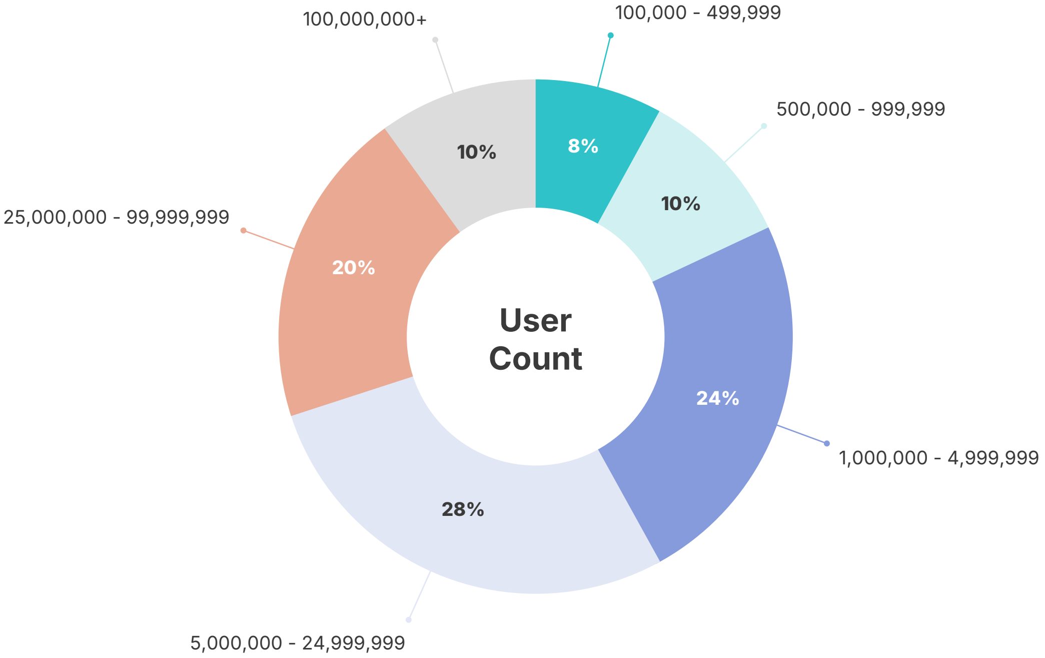
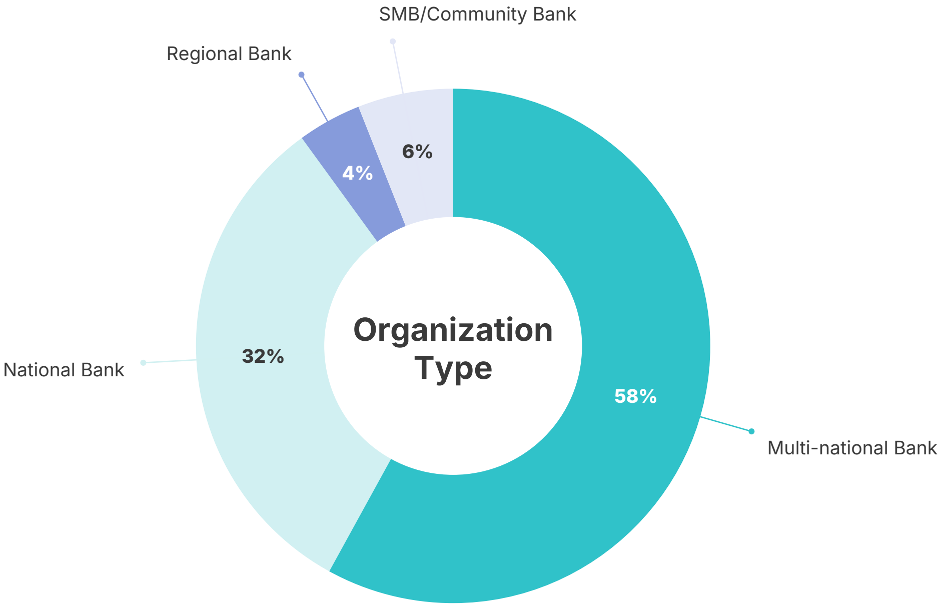


Figure 21: Respondents Organization Type

Q: What best describes your organization? (N=50)



Bibliography

1. Liminal Market Study, March 2024, surveying 50 banking buyers across North America, Europe, Latin America, Asia Pacific, and the Middle East.

2. Liminal's proprietary market sizing model, constructed using a bottoms-up approach, is grounded in a comprehensive assessment of the potential demand for solutions.

3. FTC (February 2024), "As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public."

4. Vercara (December 2023), "Vercara Research: 75% of U.S.Consumers Would Stop Purchasing from a Brand if it Suffered a Cyber Incident."

5. MX, "The Ultimate Bankers Guide to Financial Advocacy."

6. IEEE Transactions On Dependable And Secure Computing (January 2022), "Understanding Account Recovery in the Wild and its Security Implications."

7. The Guardian (February 2024), "Sim-swap fraud: How your bank account can be emptied by phone."

8. World Bank (March 2024). Note: The World Bank does not have complete data for all countries and territories. In that instance, we used similar regions as proxies.

9. New York Times (April 2021), "To Be Tracked or Not? Apple Is Now Giving Us the Choice."

10. eMarketer (January 2024), "Google turns off cookies for 30 million Chrome users, and that's just 1%."

11. Liminal. (May 2023). "The Rise of Integrated Identity Platforms."

Contact Information

Liminal is a global market intelligence and strategic advisory firm specializing in digital identity, financial crime and compliance, and Cybersecurity technology solutions across industries while also catering to the private equity and venture capital community. Founded in 2016, Liminal offers strategic and analytical services supporting executive decision-making at all product and business lifecycle stages. We advise some of the world’s most prominent business leaders, investors, and policymakers on building, acquiring, and investing in the next generation of solutions and technologies. We provide access to proprietary data and analysis, strategic frameworks, and integrated insights on the industry’s only market intelligence platform.

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

For information about our advisory services, market intelligence platform, or memberships, **sales@liminal.co**

For citations and media inquiries, **media@liminal.co**

To receive updates on new Liminal research, events, and thought leadership, **subscribe to our Newsletter.**

Visit **Liminal.co**

Unlock Actionable Market and Competitive Intelligence for Your Business

Discover how Link™ can transform your strategic decisions with the latest industry trends, market analysis, and vendor and buyer research. Technology buyers and providers can gain a competitive edge with access to market sizing, company profiles, competitive benchmarking tools, buyer intent signals, and sales enablement features.

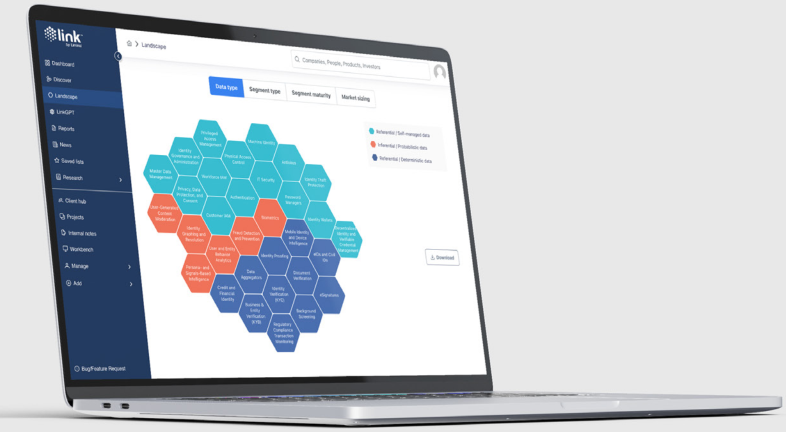
With Link™, You Can:

- Discover people, products, companies, and investments
- Explore problems, use cases, and market dynamics
- Monitor company signals in a curated and unique format
- Access research reports, survey data sets, and expert call notes
- Assess market position against peers and buyer demands
- Compare solutions to your needs
- Connect directly with buyers and vendors within the platform

Already a Member? Log in to access the report.

Join Link™ for Free Today
and Get Access to Research and More!

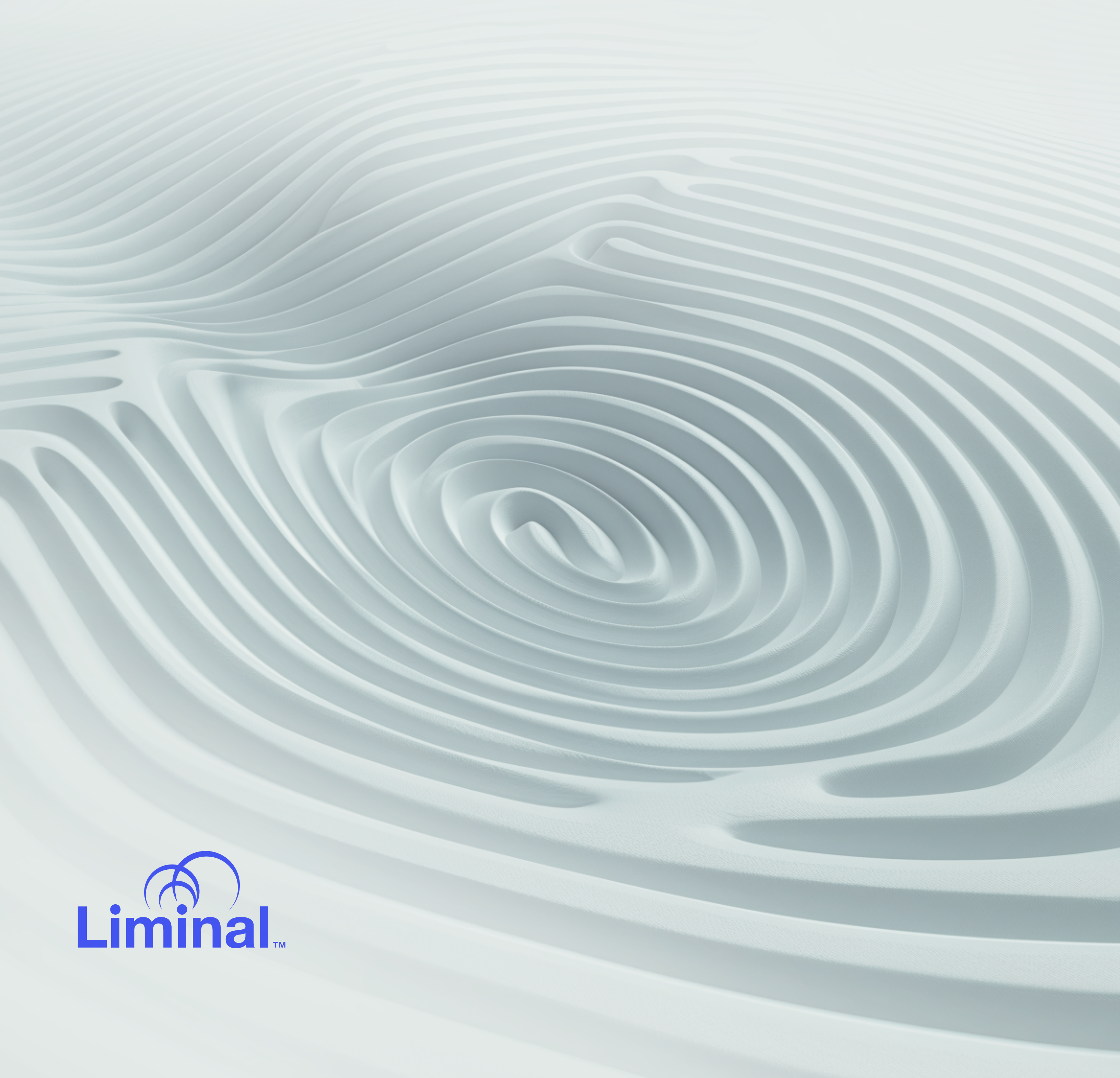
Sign Up Now


link by Liminal
Dashboard
Discover
Landscape
LinkGPT
Reports
News
Saved lists
Research
Client hub
Projects
Internal notes
Workbench
Manage
Add
Bug/Feature Request
Landscape
Companies, People, Products, Investors
Data type
Segment type
Segment maturity
Market sizing
Referential | Self-managed data
Inferential | Probabilistic data
Referential | Deterministic data
Privileged Access Management
Machine Identity
Identity Governance and Administration
Physical Access Control
Antivirus
Master Data Management
Workforce IAM
IT Security
Identity Theft Protection
Privacy, Data Protection, and Consent
Authentication
Password Managers
User-Generated Content Moderation
Customer IAM
Biometrics
Identity Wallets
Identity Graphing and Resolution
Fraud Detection and Prevention
Mobile Identity and Device Intelligence
Decentralized Identity and Verifiable Credential Management
User and Entity Behavior Analytics
Identity Proofing
eIDs and Civil IDs
Persona- and Signals-Based Intelligence
Data Aggregators
Document Verification
Credit and Financial Identity
Identity Verification (KYC)
eSignatures
Business & Entity Verification (KYB)
Background Screening
Regulatory Compliance Transaction Monitoring
Download

link™ by Liminal

Liminal™

liminal.co



Liminal™