

# Importance of Adaptive Authentication in Financial Services

The accumulation of data by enterprises and the growing number of cyber-attacks have made adaptive authentication imperative to protect valuable assets.

## **TABLE OF CONTENTS**

<b>Introduction</b> .....	<b>2</b>
<b>Current Security Challenges within Financial Services</b> .....	<b>2</b>
<b>The Need for Strong Authentication</b> .....	<b>3</b>
<b>Adaptive Authentication for Your Workforce</b> .....	<b>5</b>
<b>Adaptive Authentication for Your Customers</b> .....	<b>6</b>
<b>Conclusions</b> .....	<b>6</b>
Securing Workforce Access .....	<b>7</b>
Protecting Customer Access .....	<b>7</b>
Access Management is Dynamic .....	<b>7</b>

## INTRODUCTION

### WHY IS ADAPTIVE AUTHENTICATION AN IMPORTANT SECURITY TOOL

for financial services organizations? The accumulation of data by enterprises and the growing number of cyber-attacks have made adaptive authentication imperative to protect valuable assets. Companies must know and monitor who is accessing what, the time resources are accessed, and how the resources were accessed. Companies are slowly adopting adaptive authentication to appropriately grant to their users (employees, partners, customers) the right access. This whitepaper looks to address the challenges of securing users' identity within financial organizations, and attempts to bring to light solutions to these challenges.



**213 billion financial transactions in 2016 and 236 billion in 2017 in the US.**

### Current security challenges within financial services

Financial services enterprises are among the most targeted by bad actors or cyber-attacks. According to the Federal Reserve, there were approximately 213 billion financial transactions in 2016 and 236 billion in 2017 in the US<sup>1</sup>. These transactions were made with Debit Card, Credit Card, and prepaid cards. The constant growth of these transactions from 2012 to 2017 is depicted on the following page. As shown, people are increasing likely to pay with credit and debit cards avoiding the use of cash and checks, which puts the sensitive payment information into the hands of banks and credit card companies. Coupled with the growing world population and the demand for financial products on digital platforms, the vulnerability of financial transactions will continue to grow. These daily digital transactions are now being exposed to more threats than ever before.

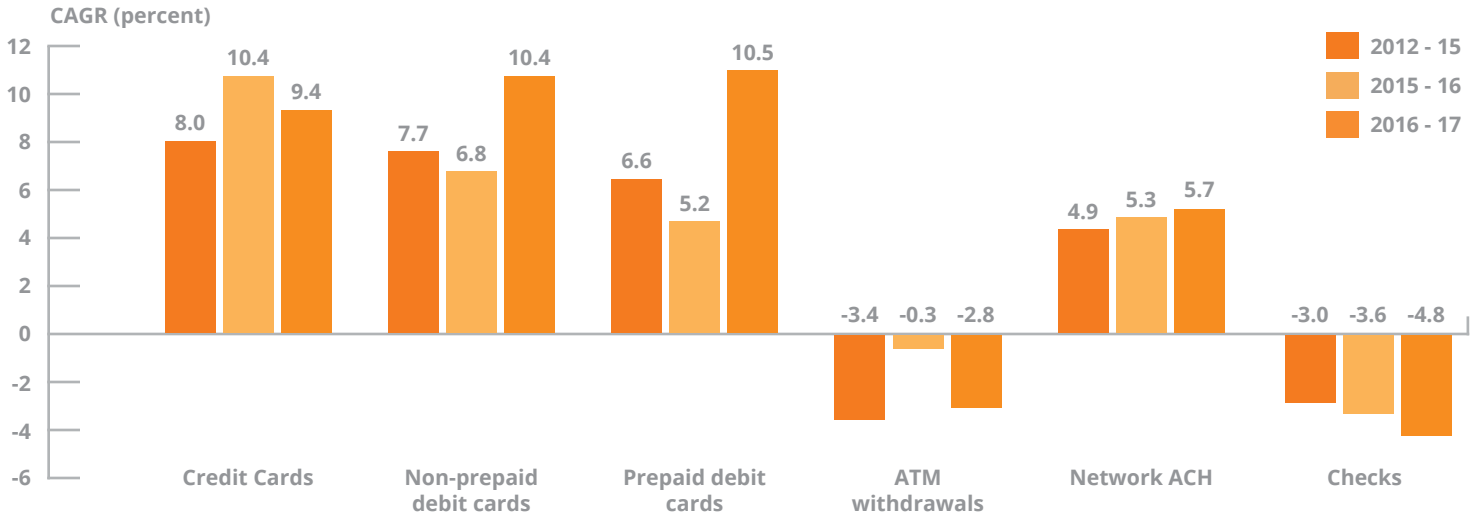
While cyber-attacks affect all industries, the business and financial industries are disproportionately impacted. According to the Identity Theft Resource Center, they both represent more than 50% of all breaches in 2019. Last year, there was an average of 108 breaches per month for the financial services industry in the US, which represented an average of 100 million sensitive records for each of those months.

Data breaches lead to both brand reputation damage and compliance issues. It's imperative for financial companies to protect themselves from bad actors to remain in compliance with local and federal regulations. Under the Know Your Customer (KYC) procedures and Bank Secrecy Act, financial institutions are required to

<sup>1</sup> [The Federal Reserve Payments Study: 2018 Annual Supplement](#)

collect and store important information such as Social Security Number (SSN), full names, address, employment status, and previous business and financial activities. The accumulation of so much sensitive and private information by financial companies has led to the enactment of policies to set guidelines on how companies should handle this data. The Right to Financial Privacy Act for instance gives the customer of a financial institution the right to some level of privacy. Banks have the obligation to protect clients' records<sup>2</sup>. The Gramm-Leach-Bliley Act requires financial institutions to explain how they share and protect customers' information<sup>3</sup>. Finally, the California Consumer Privacy Act (CCPA) also mandates the protection of customers' digital information<sup>4</sup>.

**Annual growth rates by payment type, by number and value, 2012-2017**



## THE NEED FOR STRONG AUTHENTICATION

In order to protect their brand reputations and remain in compliance with state and federal regulations, many financial institutions have implemented two-factor authentication (2FA) and multi-factor authentication (MFA) to confidently secure access for their workforce and clients. However, simple passwords and 2FA are no longer enough to protect enterprise infrastructure. Passwords are easy to compromise because they are easily predictable; therefore, they do not represent an effective barrier to bad actors. Four out of five people reuse the same password across different accounts creating potential risk for all accounts if the password is compromised. While 2FA is a good step towards better identity and access management, and an improvement over password-only authentication, there are still limitations with 2FA. For example, knowledge-based questions and answers can easily be socially engineered, hard tokens can be compromised, popular push notifications have been routinely falsely accepted, and one-time passcodes delivered via SMS/text can be spoofed<sup>5</sup>.

<sup>2</sup> [The Right Financial Privacy Act](#)

<sup>3</sup> [The Gramm-Leach-Bliley Act](#)

<sup>4</sup> [The California Consumer Privacy Act \(CCPA\)](#)

<sup>5</sup> [SecureAuth: Move Beyond Two-Factor Authentication](#)

## Many 2FA methods can be bypassed by attackers



**OTP via SMS/email**



**Phone fraud is on the rise**



**Hard Tokens**



**High Cost, Poor UX;  
compromised in the past**



**Knowledge  
Based Answers**



**Easily phished or  
found on social media**



**Push-to-Accept (P2A)**



**User conditioned to accept  
when not authenticating**

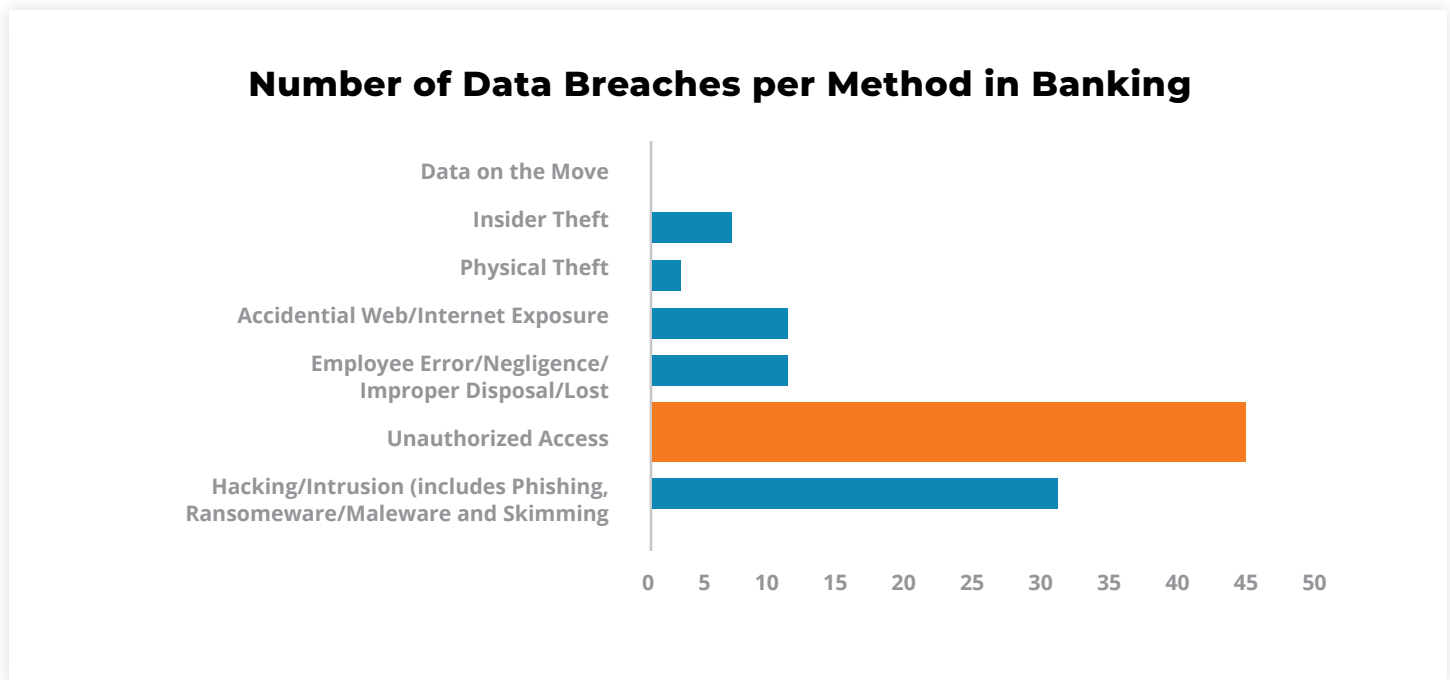
While 2FA methods were once secure processes of authentication, today's financial institutions require more sophisticated solutions to protect against cyber-attacks. To address the shortcomings of 2FA, adaptive authentication has become the new standard. Adaptive authentication adds an additional layer of security to SSO and 2FA based on factual contextual information related to the user requesting access to resources, such as a portal or applications. Adaptive authentication is a method for implementing or selecting the appropriate factors depending on a user's risk profile and tendencies. These risk-checks occur in the background and are 'invisible' to the user enabling improved security and a good user experience.



**“Adaptive authentication adds an additional layer of security to SSO and 2FA based on factual contextual information related to the user”**

## ADAPTIVE AUTHENTICATION FOR YOUR WORKFORCE

Many financial institutions are seeking to strengthen end-point security, protect their brand reputation, and meet compliance requirements. These institutions are looking for a solution that can provide a secure and seamless authentication experience to their users.

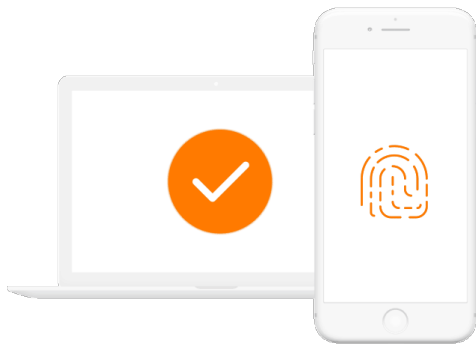


The Identity Theft Center reports that in 2019, nearly 50% of data breaches were realized through unauthorized access. An unauthorized access occurs when bad actors gain access to an environment via various forms of hacking. Bad actors exposed approximately 142,220,540 sensitive records across all industries. Unauthorized access represents the largest form of data breaches within the financial services industry. Bad actors are taking advantage of weak security systems to penetrate enterprise environments. With the sprawl of identities, data stores, deployment models, geographies, applications and devices, financial institutions should strongly consider a modern identity and access management solution to meet their security requirements while supporting their digital transformation journey. Depending on security requirements, business objectives, user experience, and current infrastructure ecosystem, financial organizations can assess and determine an IAM solution best suited for their requirements be it on-premises, in the cloud, or a hybrid approach.

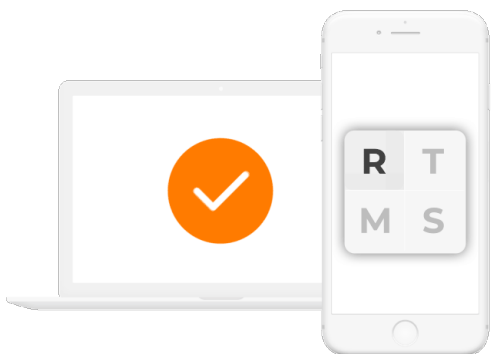
Financial organizations with a flexible and pragmatic approach to identity access management can use the platform to accelerate the adoption of new technologies, increase security, and meet the organization's digital transformation goals. In addition, these organizations will also reduce operating costs by decreasing the helpdesk burden and simultaneously improve the user experience and their productivity.

## ADAPTIVE AUTHENTICATION FOR YOUR CUSTOMERS

Beyond employees, financial institutions also have customer identities to manage. While these identities do not have access to the whole internal network, they still need to access their accounts and other personal data. Customer activities can increase the level of the company's vulnerability. Financial institutions do not only protect their internal network from bad actors, but they also need to make sure they are granting access to the right client.



**Biometric Authentication**



**Symbol-to-Accept**

Customer identity management is the foundation of any digital transformation project. Securing the identities that connect to your business enables velocity in achieving your digitization goals. For financial organizations to deliver a unified and engaging customer experience across all their digital properties, a dynamic IAM solution is required which is continuously tuned, updated, and improved to deliver the experience consumers demand for easy and secure access. Providing your customers with secure choices to access their personal data is critical for providing a positive user experience. Biometric MFA, adaptive authentication, and self-service give your customers the sense of control and protection they demand and the security your business requires. Implementing fraud and breach protection will keep your customers safe, without disrupting their user experience. A purpose-built IAM solution will focus on securing the user's identity utilizing adaptive authentication risk checks, multi-factor authentication, single sign-on, and user self-service to enable engaging customer experiences that are consistent and secure across all channels and applications.

## CONCLUSIONS

For financial services organizations, and all business, security is a priority. And the balance between strong security and a good user experience is crucial to on-going business success and competitive advantage. Ensuring organizations have a unified and pragmatic approach to Identity and Access management is essential to ensuring the security of corporate assets and the protection of the company brand. Disrupting users to achieve secure access is not an option and the cost of a poor experience may result in lost productivity, poor engagement, or lost revenue. Ensuring no unnecessary compromise exists between security and the user experience requires a breadth of options including passwordless authentication to protect resources and deliver the perfect user experience every time.

## **Securing Workforce Access**

Employees, partners and contractors are all prone to human-error and can be viewed as the weakest link in any security program. Vulnerability to phishing attacks and weak password management are two of the leading methods attackers utilize to prey on these individuals – especially because so much personal data is easily available online. And once inside an organization, bad actors can move laterally, escalating user privileges to gain access to systems and data. Deploying an IAM solution leveraging a layered approach to security ensures valuable corporate resources are available to the appropriate identity at the right time with the least amount of friction. An ability to construct authentication workflows capable of supporting a variety of use cases from simple to uniquely challenging is a foundational requirement to meet both the security requirements and the expectation surrounding the user-experience.

## **Protecting Customer Access**

Because customers connect their digital identities to financial organizations through applications, portals and other systems, these organizations must improve interactions and the user-experience in order to capture and retain customers. Financial organizations are faced with the need to ensure secure access for all customer identities engaging with their business. While at the same time preventing fraud and delivering an engaging and low-friction customer experience that increases adoption and drives better user engagement to accelerate business. Digital transformation is a top priority for most financial organizations and delivering an exceptional customer experience is critical to the success or failure of these initiatives. By delivering a secure and simple login experience, financial organizations can avoid unnecessary compromise between security and the user-experience while protecting valuable corporate assets and the company brand.

Traditional access management security architectures were designed for an era that is rapidly evolving and no longer provides the dynamic secure access requirements for today's digital business. With the introduction of SaaS offerings and other cloud-based services, the complexion of an organization's corporate resources has changed. And due to this digital evolution, a new approach to identity and access management security is required in order to meet the business and security requirements for financial organizations and their users.

## **Access Management is Dynamic**

Identity and Access Management is not a one-size-fits-all proposition. Many organizations both large and small struggle with Identity and Access Management as a program of ongoing integration. Key to long-term success for financial services organizations is understanding the strategic value of an IAM solution in the context of business operations. Security leaders with a clear view of how an IAM solution supports the business can appropriately apply resources for measured success and push for continuous improvement.

Over the past decade, Identity and Access Management has transitioned from an IT-centric administration and compliance tool to a critical security component in the modern digital enterprise. Protecting the business and supporting a rapidly expanding definition of users, a modern IAM solution must secure valuable resources, support multiple use cases, be easy to use for both administrators and users, provide intelligence, and manage the authentication of multiple user types - the workforce, contractors, partners, and customers. There is no doubt that Identity and Access Management is a requirement in today's digital world to secure, protect, automate, and enhance an organization's business operations.

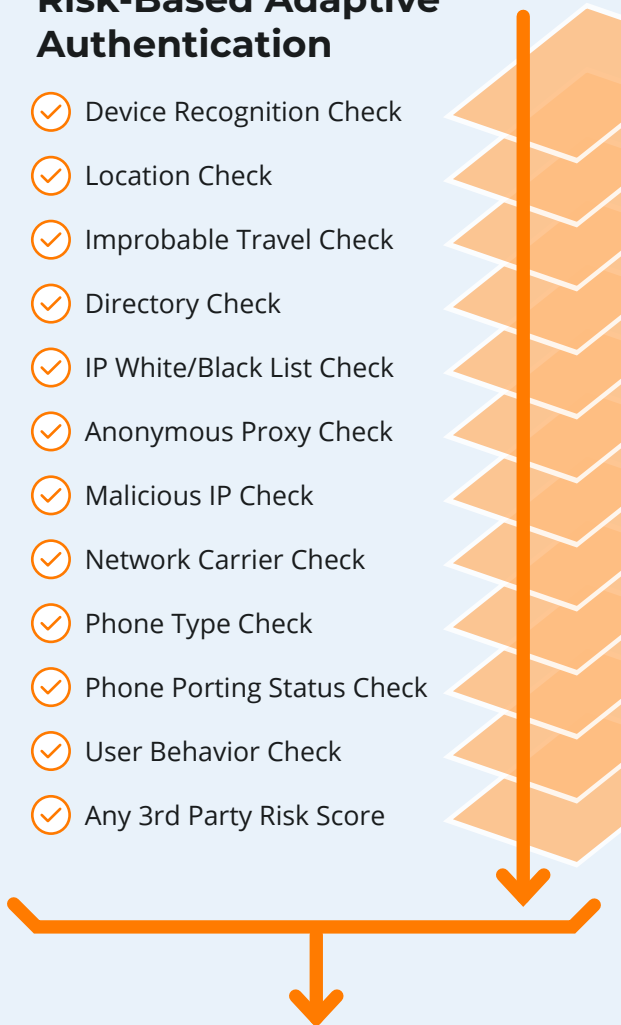


# THE SERCUREAUTH IDENTITY PLATFORM

## The SecureAuth Identity Platform Delivers

- **The most multi-factor authentication methods** – provide options and choices for users while security professionals meet more use cases and conquer security concerns
- **The most adaptive authentication risk checks** – protect your organization while preserving experience with behind the scenes risk analysis that will not burden users
- **The most federation protocols** – deliver a unified and seamless user experience for all your workforce identities
- **Infinite authentication workflows** – our highly flexible workflows enable the creation of authentication experiences that meet the security and usability needs of every workforce identity
- **User self-service options** – self-service features for password resets, account unlocks, device enrollment and profile updates mean users stay productive and you reduce helpdesk calls delivering an immediate return on investment
- **Deployment freedom** – deploy any way you want — hybrid, on-prem, or cloud — our platform delivers the flexibility enterprises need
- **Simple administration** – globally managed configurations and policies combine with an extensive application template library to enable rapid creation and easy management of authentication experiences
- **Intelligent Identity Cloud** – cloud-based analytics and administration that employs a big-data approach to delivering identity intelligence that informs adaptive authentication to ensure strong security and maximum usability for all your identities.

### Risk-Based Adaptive Authentication

- ✓ Device Recognition Check
  - ✓ Location Check
  - ✓ Improbable Travel Check
  - ✓ Directory Check
  - ✓ IP White/Black List Check
  - ✓ Anonymous Proxy Check
  - ✓ Malicious IP Check
  - ✓ Network Carrier Check
  - ✓ Phone Type Check
  - ✓ Phone Porting Status Check
  - ✓ User Behavior Check
  - ✓ Any 3rd Party Risk Score
- 

To learn more about the value of SecureAuth, please visit [www.SecureAuth.com](http://www.SecureAuth.com)