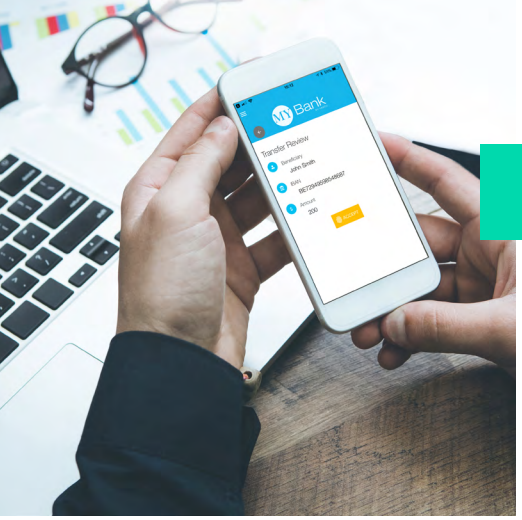
OneSpan
Be bold. Be secure.

ADAPTIVE AUTHENTICATION SUPERIOR USER EXPERIENCE AND GROWTH THROUGH INTELLIGENT SECURITY

WHITE PAPER

TABLE OF CONTENTS

Executive Summary	3
Introduction	4
Challenges with Standalone MFA Methods	6
The Current State of Authentication	8
What Is Adaptive Authentication?	9
What Is Driving Adaptive Authentication Adoption?	11
Unique Value and Benefits of Adaptive Authentication	12
OneSpan Intelligent Adaptive Authentication	13



EXECUTIVE SUMMARY

The typical mobile and online banking attack surface has greatly expanded over the past several years. In response, authentication must be portable, persistent, and flexible enough to handle the growing complexity of the digital age. Banks and financial institutions must contend with the vast array of mobile devices, multiple channels, and the customer's expectation to interact with applications when, where, and how they choose.

There are two trends impacting the marketplace at the same time. On the one hand, the need for strong authentication and security continues to rise. Fraud and hacking attempts only grow in sophistication year after year, and escalating regulation demands stronger means of authentication and risk analysis. New tools are necessary to combat these fraud attempts and remain in compliance. But on the other hand, the user's patience for additional security measures is dwindling. That leaves banks and other businesses in a no-win scenario. They risk either alienating their customers or leaving them vulnerable to fraud and attack.

To make a difficult challenge even more so, banks and financial institutions have been unable to leverage a single, comprehensive solution to mitigate fraud and improve usability for end users. Instead, they have a patchwork quilt of different tools and technologies from different vendors that were never meant to interoperate.

In this white paper, we review the historical context that has moved the industry towards adaptive authentication as well as the benefits and considerations surrounding its implementation by banks.

Key Findings

- Adaptive authentication is key to unlocking growth for banks by improving the user experience across channels. This can be done with frictionless authentication facilitated by better fraud detection and mitigation through sophisticated machine learning and customized rule sets.
- Behavioral biometrics and mobile apps will both play important roles in adaptive authentication, and the former will be leveraged more extensively going forward to preserve a more frictionless user experience.
- The days of distinguishing between weak and strong passwords are over; every password is vulnerable, as breaches and password reuse rise.
- Authentication orchestration and automation tools will be more critical as businesses need to better integrate multiple identity systems and respond in real-time to threats.
- Strong authentication needs to be delivered to users across all digital devices and channels.
- Banks continue to look for ways to reduce costs and unlock efficiencies by rationalizing authentication and fraud technologies. This can be achieved by simplifying integration and ongoing maintenance requirements through the use of more open and modular platforms.

Introduction

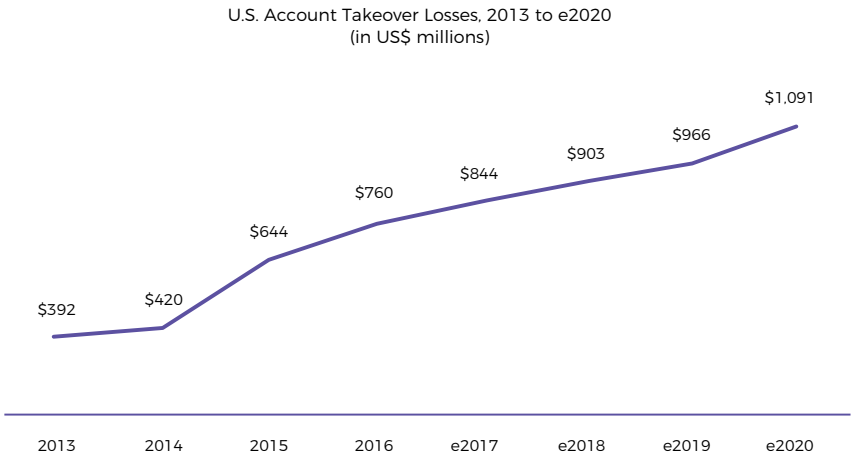
Whether you call it risk-based, adaptive, or step-up authentication, the technology is here to stay, and the old days of having a simple and static username/password pair for your logins are pretty much over. This is thanks to increases in online fraud, account takeovers, stolen and compromised passwords, phishing, and other social engineering attacks. The terms have been around for decades and are mostly used interchangeably to reflect the way a user is granted access to a particular account and its features are no longer a binary on/off state.[1]

Fraud is certainly a big business resulting in tens of billions of dollars in losses annually. Financial services firms are reportedly hit by security incidents three times as often as businesses in other sectors.[2]

Part of the problem is that financial firms have complex computing environments that are only growing in complexity as they incorporate new technologies, and as a result, these environments are becoming harder to defend. One study shows that the average bank had 30 domain configuration issues, 42 SSL configuration issues, 87 IP reputation issues, and 81 threat indicators across their digital footprints. That is a lot of different touch points to monitor and maintain.[3]

Verizon found in its "2017 Data Breach Investigations Report"[4] that 81 percent of all online breaches resulted from stolen or weak passwords. And IDC stated in the 2016 report, "The Era of the Password Has Passed," that "continuing to use the password for authentication unfairly shifts the responsibility for security from IT and security professionals to end users."[5] When fraud happens and a customer's identity is stolen, there are big implications for financial services firms. In a 2016 survey of identity theft and fraud victims, 12 percent of respondents left their credit unions, 28 percent left their banks, and 22 percent left their credit card companies as result of unauthorized activity on their accounts.[6] The trend in losses due to account takeovers continues to climb, as shown in this graph below from the Aite Group.[7]

Figure1: U.S FI ATO Fraud Losses



Source: Aite Group

So the stakes are high and getting higher as the potential for fraud dramatically rises. To make matters more complicated, achieving the right balance of security while maintaining a positive user experience is a continued challenge for security managers at most organizations. Add too many authentication layers, and users will get frustrated or consume unproductive time trying to gain access to their accounts. Have too lax a collection of authentication policies, and you'll end up with a fast growing list of customers with compromised personal information that will surely be used for theft/fraud.

And this is where adaptive authentication comes into play and why more financial institutions are adopting it.

Part of the problem with binary static passwords is that the methods behind fraud-based attacks are so sophisticated that a simple password has no hope of preventing them. These attacks can make use of a variety of malware tools to penetrate a network, establish themselves across various servers, and use different methods to compromise user credentials, disable various protective measures, and hide from detection.

For example, malware can steal a user's credentials, log in to the victim's account via a web browser, and then prepare to aid the attacker in the next phase. Meanwhile, the attacker calls a help line, uses social engineering to impersonate the victim, and sets up the attacker with new credentials. These types of attacks can cut across a website, a mobile app, call center, and legacy on-premises applications, making them very hard to track if viewed as separate and independent events.

Challenges with standalone MFA methods

Before we talk about adaptive authentication, we need to provide some historical context around previous authentication strategies. By understanding the journey authentication technology has traveled, we can better understand the role of adaptive authentication today.

In the mid-90s, multi-factor authentication (MFA) was the best method of ensuring that a user had legitimate access to an application and could authenticate properly. The idea was that any one piece of information can become compromised by a fraudster, but if you request multiple pieces and multiple types of information, the likelihood of fraud would be far lower. For that reason, MFA at the time consisted of "something the user knows," coupled with "something the user has or is".

Banks used to rely solely on MFA methods to provide solid foundational security, but due to advances in fraud, malware, and attack strategies, the cracks in the foundation are beginning to appear. Today, the right level of security requires additional technologies to keep up with the emerging threat vectors.

MFA isn't immune from being compromised. Text messages sent to a user's phone, for example, could have been hijacked, spoofed, and subject to attack. One of the biggest trends in defeating several forms of MFA methods is using real-time phishing and social engineering techniques that compromise a user's SMS or phone number to obtain the second factor passcode.

Organizations tried to address these challenges by introducing more and more biometric and advanced authentication techniques for mobile devices. The goal was to replace their outdated password-based authentication with more innovative, user-friendly, and secure alternatives.

While that was heading in the right direction, just having more factors to authenticate a user doesn't always provide the right level of security for an application or an optimal user experience.

Leading vendors began to couple MFA with risk analytics engines to provide a more flexible approach to authentication, and this strategy holds true today. Standalone MFA methods aren't rendered obsolete by new threat vectors, but they can no longer act in isolation. They should be part of a more holistic authentication solution.

However, risk scoring strategies are not all the same. They have been around for years and require modernization as well. In the past, risk scoring would assign a value to transactions (e.g., from 1 to 100). The higher the number, the higher risk of fraud the transaction posed.

Unfortunately, this simplistic approach doesn't factor in the wide breadth of circumstances in which users find themselves these days. The world is complex; a user can have multiple smartphones, a laptop, a tablet, and a desktop computer to access their digital life. Authenticating all these devices isn't a straightforward process anymore. New methods are needed to effectively assess and score multiple situations and use cases in real time.

Because of these multiple devices, authentication can't be one-size-fits-all anymore. There are different situations, even within a single smartphone application, that must be accounted for.

For example, when a user is doing something particularly risky, such as a funds transfer or adding a new payee to their online banking account, authentication must become more comprehensive. Similarly, if a user logs into their account from a new browser or device, the organization needs to verify whether it really is the user and not some hacker trying to spoof that account. In both instances, a simple yes or no process will not suffice.

MFA methods were also designed in an era when we had far fewer logins to deal with. Today these logins have proliferated along with the number of SaaS and cloud-based resources that the average knowledge worker needs to use. Authentication based on passwords or PINs isn't scalable or usable under these conditions. To resolve this, vendors have created efforts in support of the Fast Identity Online Alliance (FIDO). This potentially reduces the need to carry multiple one-time token generators and could be another element in an adaptive authentication system.

In addition, as users spend more time with typical consumer services, such as Facebook, Twitter, and Google Apps, they become used to a level of self-service and on-boarding ease that increases expectations for their business apps. In the IDC report, "The Death of 2FA and the Birth of Modern Authentication," Research Vice President of Security Solutions, Frank Dickson says that "Devices such as the iPhone changed the belief that technology has to be complicated to be sophisticated."[8]

However, that same IDC report dispels the notion that users are lazy. They just don't want to be forced into "unmanageable password hygiene practices or clunky and inappropriate methods for strong authentication." Users don't have the time, patience, or desire to go through extensive training and onboarding before they use a new SaaS product. They don't want to call a corporate help desk or wait on hold for someone to reset their password. Likewise, having to fumble around for an OTP token isn't acceptable anymore. Users want immediate access to services. They grow impatient if the fingerprint scanner on their smartphones takes too long to verify or if they have to retype a password because of a simple typing error.

Financial institutions have to keep up with this high level of usability in their own apps, otherwise users will take their business elsewhere. And as more smartphones are used by the general population, applications need to be designed with security front of mind and not as an afterthought.

ADAPTIVE AUTHENTICATION AT-A-GLANCE

- Adaptive Authentication is not an authentication factor, like a new one-time-token or authentication application. It is a workflow that dramatically departs from the authentication status quo.
- Adaptive authentication typically integrates a user's activities, environment, and behaviors into the security fabric to drive precise and intelligent security for each unique interaction.
- Under adaptive authentication, behavioral biometrics leverages the completely invisible evaluation of a user's device behavior to improve fraud detection accuracy.
- MFA is a part of the total adaptive package. Adaptive authentication utilizing orchestration technology, understands when to use the various authentication factors and when not to use them.
- Adaptive authentication fully optimizes the user experience, but more broadly, it ensures that the amount of friction the user experiences aligns with the level of risk for a particular transaction.

The Current State of Authentication

To make up for these deficiencies in standalone authentication solutions, banks and other financial companies are forced to purchase different parts of the authentication tech chain from various suppliers. This creates tremendous complexity as organizations license individual tools for fraud detection, biometrics, identity servers, security appliances, and more. From there, organizations try to tie things together, with frustrating results.

These tools were never intended to be used together, and integration can become expensive and cumbersome. As new authentication technologies come to market, this only grows more complex and creates new pain points for the business. While a boon for consultants, it doesn't make for more secure and usable systems.

Orchestrating all these different systems also becomes a challenge, mainly because automation doesn't usually figure into the best-of-breed solutions or can't be implemented across multiple vendors easily. Automation is also critical to reduce end-user support calls. Forrester says that risk-based authentication was made with ease of use in mind and can reduce help center call volumes on password resets and accidental account lock-outs.

Finally, the authentication technology industry operates in an evolving and ever-changing regulatory and compliance landscape. Both the GDPR and PSD2 have been very specific about the increased care in authenticating users in their latest drafts.

What Is Adaptive Authentication?

To solve some of the problems with standalone authentication tools, vendors developed adaptive authentication solutions.

Adaptive authentication distinguishes itself from standalone authentication tools by employing specialized authentication methods based on a real-time risk landscape. Instead of forcing a user-initiated event, such as typing in a PIN or passphrase, a user may have to pass through a series of security gates to gain access to particular services or actions for riskier interactions or no additional gates at all for lower risk interactions.

However, these security hurdles involve a variety of technologies seamlessly integrated into the background of the application. The user may not even be aware that their location, environment, biometric data, keyboard cadence, and more are being compared to a historical profile of how they normally interact with the application. Instead of a binary pass/fail action, a user is being continually assessed without their direct participation. Only when the user's behavior deviates from this normal activity will the adaptive authentication technology intervene and trigger additional layers of security.

The end result is a system in which the user has to pass increasingly secure hurdles to gain access to sensitive accounts or riskier actions, such as bank wire transfers versus a balance inquiry.

The technique has four key differentiating factors from previous static authentications:

Automated Risk Profile and Assessment Tools

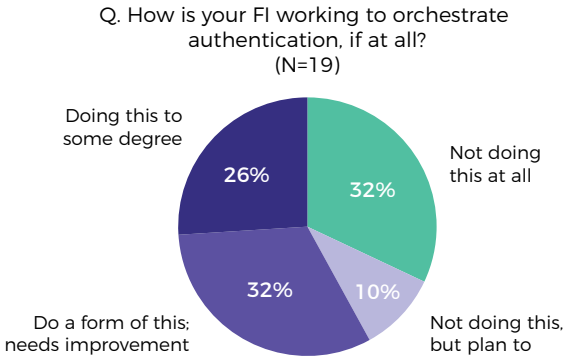
Adaptive authentication works through an understanding of user behavior, device integrity, and other contextual inputs. Though the software may not know your current bank balance or the date of your last car payment, it will recognize that you regularly transfer $200 to the same account each month from the same mobile phone in Chicago. The data is based on your activity rather than static knowledge about your finances and personal life.

Why is this information important? Because, if it now appears that you're trying to send $1,000 to a new account from a different device in New York, this falls outside your usual scope and contextual pattern. As a result, this transaction is more likely to be an attempt at fraud, but people don't live in boxes. It's entirely possible that you traveled to another city for the weekend and needed to complete this transaction. Therefore, instead of denying the transaction, the adaptive authentication tool challenges you accordingly. You get conditional access to particular account features, such as the larger funds transfers. If you can pass the security hurdle and authenticate, you can proceed with your transfer as normal. As your particular contextual patterns and circumstances evolve, the solution is intelligent enough to recognize these changes in your habits and adapt.

As part of this process, adaptive authentication assembles a series of risk scores to evaluate these various situations. But unlike the older, linear scores, it can cover multiple dimensions and circumstances and change moment-to-moment. The adaptive risk score can then become more accurate as it accepts these various third-party inputs. It will become a more reliable indicator of account compromise and potential fraudulent access over time, and because it is based on your unique usage patterns, it can be very difficult to impersonate.

A large part of this automation process is orchestrating how adaptive authentication will be used and how these assessments will be carried out by the suite of applications that an organization ultimately chooses to deploy. The best orchestration technology can examine a wide variety of inputs and combine everything together to make a real-time decision about the precise level of authentication security to apply to each unique interaction.

Figure 2: Status of Orchestrating Authentication



Source: Aite Group interviews with 28 fraud executives from 19 large North American FIs, July to September 2017

In a study from the Aite Group titled "Digital Authentication: New Opportunities to Enhance the Customer Journey." (see Figure 2), many executives report that they are overhauling their authentication strategies across all channels and looking for ways to strengthen them while minimizing customer friction. This is critical when personal information is easily available to fraudsters, because automated and organized attacks are increasing and payments are rapidly evolving to become faster or real time. Cross-channel behavior analysis is required to identify the most-complex fraud attacks; however, most online fraud detection solutions (including those applying machine learning) are still focused on point solutions for specific channels. [9]

Real-time Analysis

For adaptive authentication to be successful, it has to happen in real time. It isn't just making a single assessment when a user logs into their account but continuously monitoring as the user interacts with the application, moves about the world, and changes devices in their daily computing lives.

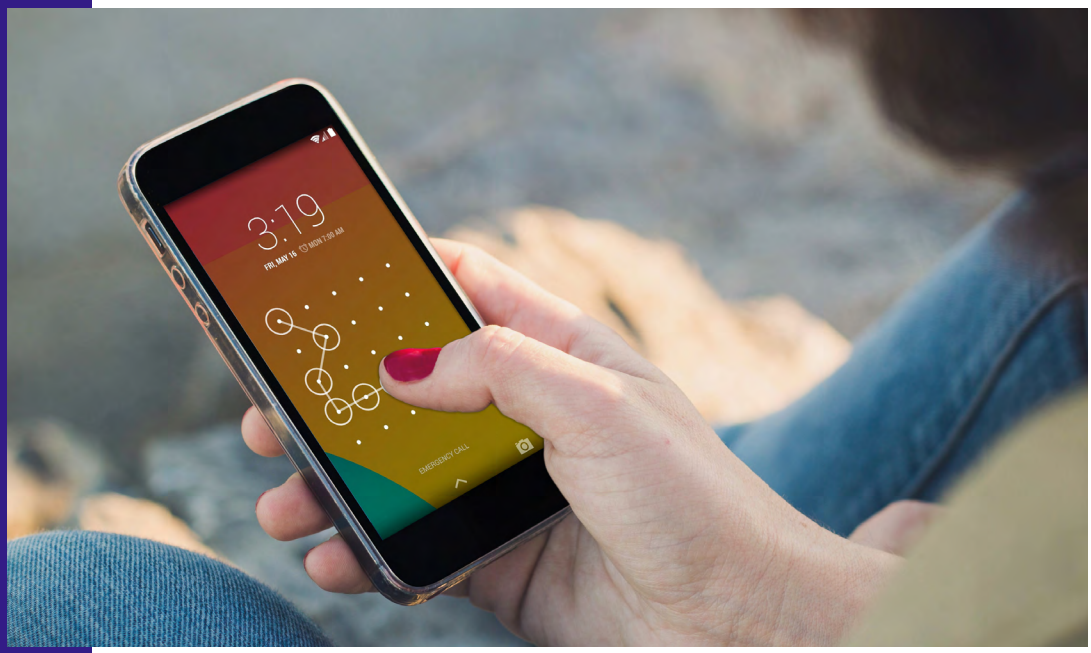
In the past, users were authenticated once per session. Controls were put into place to detect user inactivity and to set a timeout period that would automatically log them out once this period was exceeded. Today, that strategy is too crude. This one-time access doesn't really deter hackers or fraudulent use of accounts. Instead, organizations need a continuous assessment of what the user is doing and how that matches a particular profile of past behavior.

For example, adaptive authentication uses geo-location and movement velocity data in its assessment of the user. If a user first accesses the account in New York and then again ten minutes later from Paris, it is clear that these are two different individuals using the same account. Traditional authentication methods would be unable to recognize this anomaly and equally unable to respond in real time.

A critical dependence on behavioral biometrics

Adaptive authentication also leverages how the user behaves with their device, so that the device becomes part of the risk assessment and authentication process. The ways in which we move our mouse, swipe on a keypad, hold our phone and interact with our applications turns out to be quite predictable and can be used to supplement other contextual data for more accurate fraud detection.

What's important here is that these biometrics are much more than just recognizing a fingerprint or face. It is more about the continuity of the interaction, not just a pass/fail at a specific point in time.



> The key to successfully deploying these technologies without disrupting the user experience is to ensure that solutions are well-integrated, not additive. Any friction should be appropriate for the risk of the transaction. The good news is that a variety of technologies are now available that can bring both greater security and a superior user experience.
>
> **Julie Conroy, Research Director, Retail Banking and Payments Aite Group LLC**
> [10]

What Is Driving Adaptive Authentication Adoption?

Adaptive authentication has four key drivers that make it more useful to banks and other financial institutions. The first driver is to **improve the overall customer experience and retain existing customers**. For years banks have struggled to balance security in their web and mobile apps. Adaptive authentication provides an opportunity to achieve this goal and make new apps easier to use while still providing the right level of security. As banks add new online services and new ways to serve a more mobile population, adaptive technologies can help them keep pace with security and provide the least intrusive experience possible for their customers.

Second, there are **numerous compliance reasons as we mentioned earlier.** US and EU regulators are responding to the numerous data breaches due to compromised passwords by placing more specific regulations regarding authentication on financial institutions, and adaptive methods and tools can help satisfy these requirements.

Next, it **simplifies the complexity of numerous legacy technologies** that have been acquired over the years by banks and others. Because these technologies don't interoperate with each other, banks and financial institutions need a way to unify authentication decisions and create additional automated systems that can pass these decisions among each other without getting in the way of what their customers are trying to accomplish with their banking apps.

Finally, there is the need to continue to **improve overall security posture** as hackers grow more adept at compromising systems and attempting fraud. Authentication needs to be frictionless and easy for users and IT departments. Adaptive authentication can expand the frictionless approach by making authentication decisions happen in the background, without any active user participation, using risk analytics with machine learning and biometric methods.

Unique Value and Benefits of Adaptive Authentication

As a result of adaptive authentication's dynamic, intelligent, and precise level of security, it provides a more frictionless experience for customers of financial institutions. While considerable effort has been expended in years past to create "stronger" passwords, recent events have shown there is no such thing. **All static passwords are vulnerable** to the right series of attacks and social engineering efforts.

But, adaptive authentication also alleviates many of the other challenges that arise from static password authentication. Adaptive authentication can:

- Prevent password fatigue, where users are tempted to reuse existing passwords, because they have to manage so many manual logins.
- Manage multiple channels and circumstances, including digital, mobile, third-party apps, and a wide variety of use cases.
- Reduce help desk password-reset requests and unlocking requests from users who forget their static passwords.
- Match the account actions and associated risk with the right collection of authentication decisions to help prevent and minimize fraudulent account use.
- Ensure the bank remains in compliance with strict regulations.

OneSpan Intelligent Adaptive Authentication

Though many adaptive authentication solutions operate under the same principles, there is wide diversity in the market with regard to approach, expertise, and integration of key security technologies. OneSpan's intelligent Adaptive Authentication offers the following unique capabilities:

1. **Simplify otherwise complex authentication changes**
   A feature-rich, centralized management console has the power to establish a new authentication method for even the largest bank customer communities in just minutes. Without this capability, developers can invest days, even weeks updating applications, conducting QA testing, and relaunching the apps back into the market.

2. **Open, future-proof technology platform**
   The OneSpan intelligent Adaptive Authentication solution is built on an open, cloud-based architecture (OneSpan Trusted Identity Platform). This open platform enables easy integration of third-party fraud tools and data sets directly into the platform's risk analytics engine, to increase the accuracy of fraud detection through richer fraud data. Banks have the flexibility to integrate fraud tools and data that work best, ultimately supporting an approach tailored to their unique applications and IT environment.

3. **Orchestration technology that streamlines deployment**
   Our adaptive authentication solution offers compelling speed-to-market and deployment benefits to banks. A core element of our solution that enables faster deployment is a unique orchestration technology that streamlines the amount of development and coding required to deploy the solution. This is achieved mainly by dramatically reducing the number of API's required. The net of this capability is reduced burden on the bank's overwhelmed development teams who are constantly challenged to turn out more applications, faster, due to today's iterative, agile development processes.

4. **Designed to quickly meet regulatory compliance**
   Other features of the OneSpan intelligent Adaptive Authentication solution are designed to help banks achieve strict regulatory compliance faster and more comprehensively. Regulations like PSD2, GDPR, and PCI DSS 3.2 are quite extensive and have sizable penalties for non-compliance. OneSpan intelligent Adaptive Authentication offers features like a powerful risk analytics engine leveraging machine learning to better detect fraud and custom tailored and pre-configured rulesets specifically designed to address compliance requirements faster. These turn-key rulesets provide a significant time-saving foundation for the testing and deployment of this complete and fully compliant solution.

5. **Extensive visibility to mobile channel integrity**
   Perhaps one of the most unique features of our our intelligent Adaptive Authentication is the depth of visibility to the mobile device and bank apps running on them. OneSpan intelligent Adaptive Authentication leverages extensive user, device and app data from the mobile device including OS version, device ID, geolocation, jailbreak/rooting and application security data points, like detection of malware, all of which provide a very accurate measure of trust via a risk analytics score. A clear line-of-site to the integrity of mobile channel transactions creates trust and this is the cornerstone to bank growth via greater services utilization, higher value transactions and related customer loyalty.

6. **Operational efficiency**
   The OneSpan intelligent Adaptive Authentication solution utilizes a sophisticated user interface that provides a single point of control for many rules, workflows, and actionable authorizations. Not only does this provide an intuitive user experience, but it contributes to greater efficiency and reduced costs around authentication. Furthermore, the solution supports role-based administration that allows the bank to assign privileges to administrators based on their duties.

The Future of Adaptive Authentication

The future of adaptive authentication is indeed a bright one. It can bring better security and better usability to the application, forever removing the zero-sum trade-off between these two goals.

It can allow financial institutions to keep up with technology advances in authentication without having to scrap existing methods and investments in MFA and other access tools. It can allow for greater flexibility of smartphone application use and monitoring, without requiring the bank to be "big brother" to its customers. It can bring together tools from multiple developers onto a single, unified open architecture platform.

Most importantly, it can tie the two more closely together to reduce churn and defections, providing a strong foundation for growth.

[1] https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era

[2] https://www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks

[3] http://www.globenewswire.com/news-release/2018/02/20/1361646/0/en/RiskIQ-Announces-New-Digital-Footprint-Risk-Reporting-to-Improve-Digital-Defense.html

[4] https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf

[5] https://www.secureauth.com/sites/default/files/sa_analystreport_idc_the_era_of_passwordless.pdf

[6] http://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf

[7] https://aitegroup.com/report/digital-authentication-new-opportunities-enhance-customer-journey

[8] https://www.idc.com/getdoc.jsp?containerId=US42965617

[9] Gartner, Market Guide for Online Fraud Detection, 31 January 2018

[10] Digital Authentication: New Opportunities to Enhance the Customer Journey

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

For more information about adaptive authentication, contact OneSpan or register for our development portal.

CONTACT US

For more information:
info@OneSpan.com
www.OneSpan.com