The Future of Adaptive Authentication in the Financial Industry

Is Your Organization Applying the Right Amount of Security to the Right Transactions?
The State of Adaptive Authentication in the Financial Industry

Caught within a shifting threat landscape, a tighter regulatory environment and a seismic shift in customers’ banking preferences – and their tolerance for security – financial institutions globally are making a shift to adaptive authentication. This is the process of applying the precise amount of security, at the right time, to each unique customer transaction based on the level of risk.

What’s driving this shift? What are the necessary tools and skills? What are the business benefits, as well as the obstacles that could impede the move to adaptive authentication?

These questions are among those to be answered in this State of Adaptive Authentication in the Financial Industry survey. Here are some highlights:

Fifty-five percent of survey respondents say their institution’s digital authentication measures are average or below when compared to their peers. And 55 percent rate themselves at average or below when it comes to their institution’s current ability to apply the precise amount of security to the right transactions at the right time.

With responses from more than 150 respondents from primarily U.S. institutions, the survey finds that only 37 percent currently have adaptive authentication as an active initiative. But 44 percent say adaptive authentication will be an active initiative in 2019.

Among some of the other key findings:

- **Fraud Stats:** Seventy-nine percent of respondents say the number of fraud incidents has remained steady or increased over the past year, while 69 percent say the fraud losses associated with these incidents have remained steady or increased.
- **Improving Authentication:** Ninety-three percent of respondents say that streamlining the customer authentication experience is either one of their top authentication priorities for 2019 or their single highest priority. Forty-seven percent say their biggest obstacle to improving authentication is “our systems are tied to traditional username/password authentication processes.”
- **2019 Budget:** Ninety-six percent of respondents expect the same or more budget for authentication improvement in 2019 compared to last year. And among the top solutions targeted for investment:
  - Adaptive authentication – 40%
  - Software token – 35%
  - Behavioral biometrics – 26%

Read on for the full survey results, as well as expert analysis of how to put this information to use, to simplify the customer experience, reduce fraud and meeting regulatory compliance.

Best,

Tom Field
Senior Vice President, Editorial
Information Security Media Group
tfield@ismg.io
This survey was conducted online in the winter of 2018-2019, and it generated roughly 150 responses from financial institutions primarily in the U.S. Twenty-four percent of the respondent base was from financial institutions with $40 billion or more assets under management.

About 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. Learn more about OneSpan at OneSpan.com, and on Twitter, LinkedIn and Facebook.
By the Numbers

Some statistics that jump out from this study:

55% say their institution’s digital authentication measures are average or below when compared to their peers.

55% rate themselves at average or below when it comes to their institution’s current ability to apply the right amount of security to the right transactions at the right time.

93% say that streamlining the customer authentication experience is either one of their top authentication priorities or the top priority in 2019.
NOTE: In preparation of this report, ISMG’s Tom Field interviewed Julie Conroy, research director of Aite Group, on the results and what they mean for banking institutions. This is an excerpt of that conversation.

Results are Consistent

TOM FIELD: As a researcher looking at our survey results, what is your gut reaction to them?

JULIE CONROY: They are remarkably consistent with the recent surveys we’ve done and the ongoing discussions that we have with institutions’ executives, both on the fraud side of the house and also on the customer experience side of the house. Increasingly, authentication is a shared expense and a shared burden between those two groups because the customer experience is so impacted by either good or bad authentication.

Improving Authentication

FIELD: Julie, you speak with lots of organizations. What do you typically see as their biggest obstacles to being able to improve upon traditional methods of authentication?

CONROY: That’s easy. It’s the bureaucratic practice to get new technology into a bank. It’s going through the justification of the business case. It’s then getting in line for IT resources. It’s going through all the vendor risk management overhead. That used to be a year, and people thought it was painful. But now – especially with the vendor risk management overhead scrutiny – it’s 18 months in most cases. As fast as fraud and the cyber threats are moving, that’s just way too long a period of a time to be able to adjust.

Challenges Ahead

FIELD: Julie, based on your own research, where can organizations expect to find some speed bumps on the road to more mature adaptive authentication?

CONROY: I spoke to the big one, which is just the bureaucracy. Also, as you look at things like username/password, there is unfortunately still a comfort level among consumers. We have a lot of consumer survey data that shows that consumers still are very happy with the username/password. It’s easy. They are habituated to it. And it’s easy because most consumers are using it badly. They are using the same username/password across most of their online relationships. But changing customer behavior is really hard to do, and so the process of introducing new behavior patterns is another big challenge as we’re moving toward a more sophisticated authenticators.

“We have a lot of consumer survey data that shows that consumers still are very happy with the username/password.”
**Bullish on Emerging Tech**

**FIELD:** Now as you look across the landscape this year, what are the authentication methods and technologies that you find yourself most enthusiastic about?

**CONROY:** We’re seeing a lot of movement toward various forms of biometrics. As long as the biometric is paired with a strong device identity, which makes it much harder to move, that is something that we continue to see increasing use of. The payment networks in Europe right now ... are really pushing biometrics. I like the behavioral biometric, which is behind the scenes. And this has the benefit of being transparent to the end user, but giving some good indicators of “is this my genuine customer? Is this a fraud?” There are lots of great results with the application fraud use case in behavioral biometrics where you can understand based on the way the data is being input, for example: “Is this user familiar with this Social Security number, or are they cutting and pasting it from a page that they just bought off the dark web?” The good news is that as fast as the threat environment is moving, there are lots of great technologies coming to bear that can help with better authentication as long as we can figure out a way to help advise institutions to get them deployed in a timely manner.

**Put Survey Results to Work**

**FIELD:** As a researcher, how do you recommend that our audience use the survey findings and analysis we’re providing to them?

**CONROY:** We find with our research that we produce at Aite Group that it’s very useful as institutions are trying to make their business cases. They can use this to show: “Look at this. We are behind the curve because look at where the rest of our peers are today or where they are heading. And, you know, we’re not even going to be slow followers anymore. We’re going to be laggards.” Or conversely, if an institution has been making that investment and they are out on the leading edge, they can use survey results to help not only justify their investment, but also partner with their marketing folks and position themselves as leaders in this area.

Increasingly, the investment in these types of digital identity technologies and authentication technologies is becoming a competitive issue. Those institutions that are doing it faster and better are providing better customer experiences and will win and retain more customers in that way.
Baseline Authentication

To begin this study, respondents were asked a series of fundamental questions about their current digital authentication methods, as well as their confidence in them.

Among the responses:

- Only 10 percent believe they do a superior job authenticating customers and transactions;
- 47 percent say their biggest obstacle to improving authentication is their investment in traditional processes and controls.

Read on for full results.

How do you rate the state of your banking institution’s digital authentication measures today, as compared to what you know about peer institutions?

Respondents were unusually frank with their responses to this first question. Whereas survey takers often are overly optimistic with their answers, the majority of this group – 55 percent – rate their current authentication methods as average or below.
How do you rate your banking institution’s current ability to apply the right amount of security to the right transactions at the right time – again, as compared to what you know about peer institutions?

![Survey Results](image)

Similarly, 55 percent of respondents say their organizations are at average or below when it comes to providing “step-up” authentication – or providing the right amount of security to the right transactions at the right time.

Less than 10 percent say they are doing a superior job.

What do you see as the biggest obstacles to improving how your institution approaches authentication? (select all that apply)

![Survey Results](image)

The biggest obstacles to improving authentication? It’s a close race. Tradition – being tied to user name/password technology and processes – wins by a nose at 47 percent over technology (disparate tools) and threats (evolution of them), which tie at 44 percent.

Budget is the fourth highest response.
As for the drivers to improve authentication this year, the top response by far is “to improve the customer experience and retain existing customers,” selected by nearly one-third of respondents.

The second and third-rated options:

- Improve overall security posture (24 percent);
- Combat increases in fraud incidents and related exposure (23 percent).

The next section dives deeper into the specifics of the state of authentication at respondent organizations.

As for drivers to improve authentication this year, the top response by far is "to improve the customer experience and retain existing customers."
The State of Authentication

Some immediate takeaways from the current state of authentication:

- 96 percent of respondents still rely on usernames and passwords to some extent;
- 37 percent say adaptive authentication is a current, active initiative at their organizations.

Which is your top business driver for improving authentication in 2019?

- Reduce account fraud: 37%
- Enhance customer relationships: 30%
- Ensure regulatory compliance: 25%
- Other (please specify): 8%

Diving down deeper into motivation to improve authentication, respondents were asked to reveal their top business driver: reduce account fraud (37 percent).

The other two top business drivers are:

- Enhance customer relationships – 30 percent;
- Ensure regulatory compliance – 25 percent.

The top business driver to improve authentication is to reduce account fraud.
How does “streamlining the customer authentication experience” rate as a priority for your organization as you roll out new authentication solutions?

- It is the top priority, as we will lose customers if we do not improve their experience with us: 35%
- It is a priority, but not the top priority: 58%
- It is not among our current priorities: 7%

Security leaders debate the ongoing tension between improving security and easing the digital customer experience. So respondents were asked how much of a priority this streamlined customer experience is as they roll out new authentication solutions.

For 58 percent, it is a priority, but not the top priority. Meanwhile, 35 percent say it is the top driver.

Only seven percent of respondents say it is not among current priorities at all.

What today is your customers’ primary channel for conducting business with your institution?

- Call center, via phone: 16%
- In person at our branches: 30%
- In person at our ATMs: 3%
- Web transactions/banking: 35%
- Mobile transactions/banking: 17%

To provide greater context for analysis, respondents were asked to list their customers’ primary banking channels. It’s an interesting mix of digital and traditional means: 35 percent bank via the web, while 30 percent still do business in person at branches. Seventeen percent of customers reportedly bank via mobile transactions, with the same number opting for telephone call centers.
Has the number of fraud incidents involving your organization increased, decreased or stayed steady in the past year?

- Increased: 39%
- Decreased: 10%
- Remained steady: 40%
- Unsure: 14%

Also for context, respondents were asked about fraud. Seventy-nine percent say the number of incidents have stayed steady or increased in the past year. Meanwhile ...

Have financial losses linked to fraud increased, decreased or stayed steady in the past year?

- Increased: 25%
- Decreased: 14%
- Remained steady: 44%
- Unsure: 18%

Sixty-nine percent say that financial losses linked to fraud have remained steady or increased. Only 14 percent report a decrease.
As mentioned at the start of this section, usernames and passwords are far away the most popular form of authentication, cited by 96 percent of respondents.

Other top forms:

- Knowledge based authentication questions – 65 percent;
- Software tokens – 51 percent;
- Hardware tokens and one-time passwords – 50 percent each.
Nearly half of respondent organizations (48 percent) do not calculate the ROI of the authentication technologies they have deployed.

Of those who do, the most common ROI calculations are via:

- Fraud reduction – 39 percent;
- Regulatory compliance - 25 percent;
- Digital channel use – 21 percent.

**Nearly half of respondents do not calculate the ROI of the authentication technologies they have deployed.**
Finally, when asked about their institution’s understanding and adoption of adaptive authentication tools and processes, more than one-third said this is a current, active initiative.

Most of the remaining respondents are at various stages of understanding or deploying the concept.

Only 4 percent said adaptive authentication is not applicable to their current situation or needs.

Next, the report looks at what it will take to enable adaptive authentication in 2019.
The Road to Adaptive Authentication

There are many roads to take enroute to adaptive authentication. But they all start with resources. And the good news for this group of survey respondents: 96 percent of them expect to see the same or increased budget for authentication this year.

How will they invest these funds? Read on for details.

How do you expect your authentication budget to change in 2019?

- Increase of more than 10 percent: 11%
- Increase of 6-10 percent: 16%
- Increase of 1-5 percent: 26%
- No change: 43%
- Decrease: 5%

Strike “budget” off the list of potential impediments to improving authentication in 2019. According to the survey, only 5 percent of respondents expect a decrease in funds. Meanwhile, more than one-quarter expect increases of 1-5 percent.

Where do you expect to make your primary authentication investments in 2019? (select all that apply)

- **Tools**: New multifactor authentication technologies, including those that rely on biometrics and AI/machine learning
- **Partnerships**: Relationships with vendors that can supply and maintain the new authentication tools and/or manage relationships with other vendors who supply/maintain
- **Skills**: Personnel who have the knowledge to configure, deploy and maintain new tools effectively

Asked first to broadly list their authentication investment priorities, respondents chose tools – specifically, new multifactor authentication technologies, including those that rely on biometrics and AI/ML – over partnerships and skills.

Which tools? The next questions offers answers.
Survey Results

Which of these authentication solutions will your organization invest in over the course of 2019? (select all that apply)

Adaptive authentication solutions 40%
Software token 35%
Username and password 29%
Knowledge-based authentication questions & answers 26%
Behavioral biometrics 26%
Device ID 26%
One-time passwords (OTP) 23%
Hardware token 21%
Out-of-band verification for authentication (PIN) 18%
Out-of-band verification for transactions (PIN) 17%
Facial biometrics for authentication 17%
Fingerprint biometrics for authentication 17%
Voice biometrics authentication in call centers 14%

Adaptive authentication solutions is the winner, with 40 percent of the vote. Other top tools for investment in 2019 include: software tokens (35 percent), username and password (29 percent), and KBA, device ID and behavioral biometrics, tied at 26 percent each.
Survey Results

Will adaptive authentication be an active initiative at your institution in 2019?

Asked whether adaptive authentication will be an active initiative in 2019, 44 percent say yes, while 32 percent are unsure. Just under one quarter say no.

If you answered “yes” to the previous question, what will be primary benefits you seek in pursuing adaptive authentication in 2019? (select all that apply)

- Operational costs: Reduce help desk password-reset requests and unlocking requests from users who forget their static passwords: 81%
- User experience: Prevent password fatigue, where users are tempted to reuse existing passwords: 75%
- Regulatory compliance: Ensure the bank remains in compliance with strict regulations: 49%
- Omnichannel: Manage multiple channels and circumstances, including digital, mobile, third-party apps, etc.: 40%
- Operational costs: Reduce help desk password-reset requests and unlocking requests from users who forget their static passwords: 37%
And the survey concludes with a two-part question.

For those who said adaptive authentication will be an active initiative, what primary benefits do they seek?

For 81 percent of respondents, it's all about reducing fraud, while for 75 percent it's about enhancing the user experience. Just under half – 49 percent – cite regulatory compliance.

Again, if you answered “yes” to question #17, what do you perceive to be your primary obstacles to rolling out adaptive authentication in 2019? (select all that apply)

- Replacing legacy authentication solutions (56%)
- Transitioning without negatively impacting the customer experience (50%)
- Managing third-party technology integration (46%)
- Developing in-house skills to deploy and maintain the risk models and tools (31%)
- Choosing between on-premises and cloud solutions (22%)
- Demonstrating ROI (22%)
- Maintaining compliance with existing and emerging regulations (21%)

And asked what primary obstacles they expect to encounter, 56 percent of these respondents say the top block will be replacing legacy solutions.

For 50 percent, the issue is making the transition without compromising the customer experience. Forty-six percent are concerned about managing third-party technology integration.

Next, this report will offer conclusions about the survey results, as well as expert analysis of what these results mean – and how to use them in your own organization.
Conclusions

Given that 96 percent of respondents expect the same or more budget for authentication improvement in 2019 – and that adaptive authentication solutions are their number 1 investment target – here are some conclusions about the survey responses:

The Current State of Digital Authentication Is Dangerously Flawed

It’s clear from the survey responses that far too many institutions remain beholden to usernames and passwords for authentication – and they realize the approach is flawed. The problem is: These same institutions fear inconveniencing their customers. It’s time for security and fraud leaders to accept that there are now too many legitimate banking credentials available to fraudsters, and any digital authentication system that relies on static usernames and passwords and knowledge-based question and answer (KBA) technologies/solutions is the equivalent of leaving the vault door open. It’s beyond time for change.

‘More of the Same’ Is Not a Proactive Strategy

And “change” does not mean simply adopting SMS notifications of transactions. Fraudsters have long since learned how to intercept these messages and proceed unabated to commit fraud. For financial institutions to take a significant chunk out of fraud will require investment in risk-based adaptive authentication that involves a combination of advanced risk analytics, adaptive authentication methods, including biometrics, and mobile application security to help reduce fraudulent transactions.

You Don’t Need to Choose Between Customer Convenience and Security

It’s long been believed – and often accepted – that banking customers will always take convenience over security. It’s assumed that customers value quick access to their accounts over any kind of security measure that will confirm their identity and momentarily delay that access. That may have been true before the massive data breaches at Yahoo and Equifax. But now, when even casual consumers know their identities and credentials are readily available in the dark web, smart customers don’t mind their institutions going the extra mile to authenticate identities and validate transactions. Every transaction requires the same level of risk-based analysis. And that’s the promise of adaptive authentication – that it will provide the precise level of security to the transaction at the right time. At a time when security controls have matured, and when machine learning is fueling a new era of effective analytics, banking/security leaders no longer need to choose between customer convenience and security. They can get both.

The final section of this report provides expert analysis of how to put these survey results to work to improve digital authentication.
The Future of Adaptive Authentication in the Financial Industry

Insights from John Gunn of OneSpan

NOTE: In preparation of this report, ISMG’s Tom Field interviewed John Gunn, CMO of survey sponsor OneSpan, about the results and what they mean for banking institutions. This is an excerpt of that conversation.

Reviewing the Responses

TOM FIELD: What’s your gut reaction to the survey results?

JOHN GUNN: Much of it is what we expected. We have worked with the world’s largest banks. We talk to them on a continuous basis about the challenges they face and how they are addressing them, and there are more challenges than ever as the attack methods used by hackers increase and as the competition within the financial industry heightens.

Traditional banks and credit unions are really being squeezed from both sides. How do they deliver and secure an ever-increasing experience that wows customers and allows the institutions to track and retain them – and at the same time beat down these incredibly aggressive hackers? This report reflects a lot of what we see and gives a lot of insights. So I was delighted with the results.

The State of Authentication

FIELD: John, one of the things that struck me was how brutally honest our respondents were. If they were willing to admit that their authentication is average or below compare to their peers, what do you think they are not saying?

GUNN: I don’t think they are hiding a whole lot. I think that over the last few years, everyone in the industry has figured out we have to be open and honest and collaborative.

The hackers collaborate tremendously, sharing attack information and attack tools. And banks and credit unions have really stepped up in the last few years and changed their mindset. Their defense mechanism isn’t some proprietary secret that they want to keep to themselves; there’s this big benefit from sharing it with their peers. You see a big rise that’s coming in sharing of attack data, especially with machine learning and artificial intelligence. The more collaboration there is, the more we can win this thing. It’s a new era in fighting fraud.
“New solutions and new platforms that use risk analytics that catch fraud in real time have started to make a difference.”

Roadblocks to Improvement

FIELD: What do you typically see as the biggest obstacles to institutions being able to improve authentication?

GUNN: There are two parts of it. One is the complexity of the technology and the solutions. There are myriad choices. There are different solutions that were not designed to work together. Vendor approval takes a long time. Implementation takes a long time. And then getting it all to talk together is challenging. And that’s one of the core principles that is part of our platform.

The second part of it is the impact on the customer experience. You can accept a fair amount of fraud losses when you balance them against “what does it cost if you lose a customer if they have a bad experience?” If they can’t access their funds or complete transactions, you may lose that customer for life. So there is an understandable concern about how do we achieve both at the same time.

Business Drivers for Improvement

FIELD: I’ve got to think that there are considerable business drivers to help institutions get over these obstacles.

GUNN: Absolutely. The number one business driver is that they can measure probably down to the second what their fraud losses are, and they look at the solutions they are implementing, and it’s reached a stalemate where some institutions see fraud losses going up. Some see them going down. But the investment that they are making continues to go up, and it’s a tough situation where for the average financial institution, they are spending more to stop fraud, but their losses aren’t declining rapidly. They are just holding them in check.

Collectively, the industry is saying, “OK, where is the breakthrough? When do we get to start bringing fraud down a significant way for all of our investment? Or do we have to have to just keep spending more every year without getting some great results?” And that’s coming. We’re already seeing that by the use of platforms.

New solutions and new platforms that use risk analytics that catch fraud in real time have started to make a difference. And if we have the same conversation a year from now, which I hope we do, you’re going to see some real positive gains from the application of new technology, at least for the financial institutions that move forward quickly and adopt it.

The Case for Adaptive Authentication

FIELD: From your experience with institutions, where do you see adaptive authentication really taking off? And what do you find to be some of the successful business arguments that institutions are using to get support for this?

GUNN: I’ll start by saying it’s not a brand new concept. But you look at the technology advances of the last few years, and they’re mind-blowing. You can look at situations and say, “This is an odd time for this person to do a transaction,” or “It’s an odd transaction.” The landscape for authentication has changed, and the number of data points have just exploded.

We all know that consumers are remarkably unforgiving, especially in America, and they vote with their feet and will leave that institution. So these new solutions allow institutions to reduce false positives, identify fraud that they weren’t catching in real time and achieve those mutual goals. And that’s where authentication – the adaptive part of it – has really changed.

As we integrate large pools of data from other institutions and other sources, it just improves that ability to achieve that goal. That’s why I’m confident that in the next year or two, we’re going to really see this turnaround where financial institutions will start seeing real gains in reducing fraud for their investment.

Speedbumps in the Road

FIELD: Where would you say organizations can expect to find some speedbumps on the road to mature adaptive authentication?

GUNN: The biggest speed bump is just legacy systems and legacy processes. You still have so many institutions that rely on username and password. They may supplement it by sending a text SMS, as we’ve seen in recent news stories. But those can be intercepted. Those are hacked. Of course, username and password is phenomenally insecure, but their legacy systems were built with that. And when we go into clients … we’ve got this great technology solution, and so do our many of our competitors, but how do we make this work with their existing legacy system? Some banks are up to date, and implementation is not challenging. With others that’s not the case.

Once we get over that bump in the road, then the benefits really start to be realized.
“But to be successful, the financial institution has to be able to future-proof their solution and have a platform that they can integrate.”

Quick Wins

FIELD: Are there quick wins that organizations an focus on?

GUNN: Yes, but it depends on the organization. Those that are using outdated methods – those that are just relying on username and password, or maybe just location – they can quickly expand that. They can identify and stop a lot of fraud. ROI is easy to prove pretty quickly.

None of us can predict exactly what the next threat will be, and I can’t tell you what will be the hot new subject two years from now. AI is always going to be a part of it, but biometric authentication has been around for a while and it’s proven. In two years, who knows what it will be?

But to be successful, the financial institution has to be able to future-proof their solution and have a platform that they can integrate. They can move out of older systems or strategies, methods that aren’t relevant anymore, and they can add new ones as they come up.

Nowadays, financial institutions have invested so much implementing a new solution that it’s got to be a painful decision to move away from something they’ve implemented, even if it’s not perfect. So the future is giving them the flexibility to be able to test and use the right solutions in a matter of months and not over years when the threat profile and the attacks are changing monthly, not annually.

Putting Survey to Work

FIELD: Given everything we’ve discussed, how do you recommend our audience put these survey results to work within their enterprises today?

GUNN: Talk to the experts. There are lots of really great research firms out there. There’s Gartner, Aite, Forrester . ... And then narrow your choice of vendors to those that don’t just have this great solution right now ... but a vendor that’s focused on how they bring together multiple solutions. In the banks, many of them have developed their in-house solutions that have a lot of value. They’re getting the ROI in all of it, so that collectively it’s a much more effective solution in reducing fraud while still delivering a fantastic user experience.
About ISMG

Information Security Media Group (ISMG) is the world’s largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io