BEYOND IDENTITY

# What Brands Get Wrong About Customer Authentication

WHITEPAPER | SEPTEMBER 2022

technology leaders club

In today's digital age, customer authentication is a critical component of almost every business that exists. It serves as a product gateway impacting every customer. It's not easy to get right, and the stakes for getting it wrong are higher than ever. Almost half of customers would abandon a transaction because of authentication. On top of this, account takeover fraud is an ever-increasing attack vector for cyber criminals. Effectively managing authentication security and customer usability is now vital for modern organisations.

We invited a group of CISOs, security directors, and VPs of IT to discuss their organisation's approaches to customer authentication and more about:

- The main challenges for customer frustration
- Balancing friction with security
- Managing conflicting interests with the wider business
- Driving value and building customer confidence

Rela8 Group's Technology Leaders Club roundtables are held under the Chatham House Rule. Names, organisations and some anecdotes have been withheld to protect privacy.

## About Beyond Identity

Beyond Identity is the first and only company to provide passwordless identity management. The Beyond Identity team is composed of cyber security and identity management professionals who are passionate about restoring digital trust and building a fundamentally secure way to authenticate and authorise users while protecting privacy. By eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication, Beyond Identity is fundamentally changing the way the world logs-in.

*“Not every customer has the same level of technology or tech-savvy at their disposal”*

## Knock knock – who's there?

Customer authentication has become an unavoidable aspect of modern businesses, whether you have an online platform, a mobile app, or as is increasingly likely, both. Authentication is the front door of a digital business. It needs to seamlessly allow access for customers while keeping away the pests, but this is no mean feat as security traditionally involves a trade off with seamlessness. Understanding how this friction impacts your users and effectively balancing that alongside user experience requires an understanding of your customers, their journey, and their frustrations.

## The sticking points

Much to the chagrin of security teams, authentication is more often than not seen as little more than an inconvenience. Every hurdle a customer hits is an opportunity for them to give up, change their mind and leave. Throw in the inconsistency of authentication requirements across various apps, be they push notifications or verification codes etc., and you have a recipe for annoyed customers who are one authentication alert away from walking out.

When thinking about why customers are so frustrated by authentication it's important to remember that each user has individual circumstances to consider. Not every customer has the same level of technology or tech-savvy at their disposal, making some more sophisticated solutions unrealistic and in some cases, actual barriers to usage. Authentication can still prove an issue even for the customers more comfortable with modern security requirements. Constant alerts and requirements to authenticate can come across as immature technology which can harm the customer adoption and retention curves, in turn impacting an organisation's bottom line.

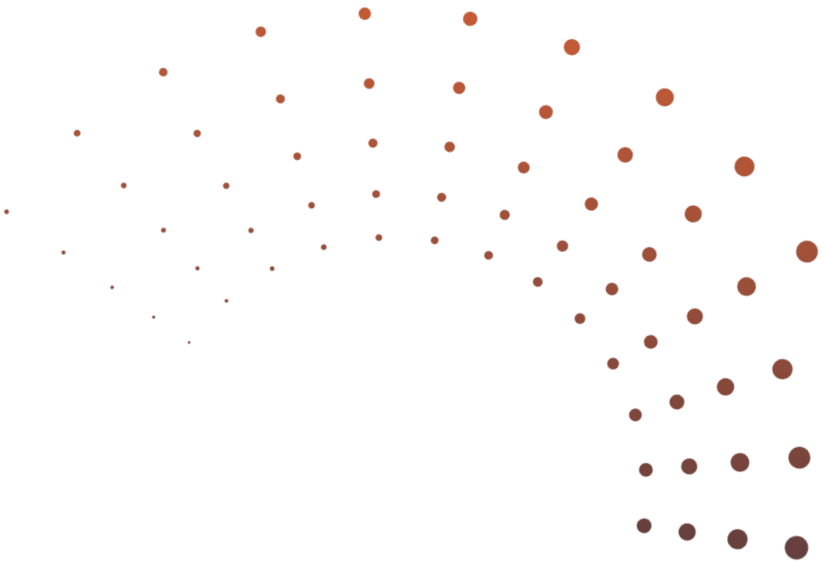
Internally, security teams will find themselves battling those who don't like the idea of moving away from "how we've always done it", as well as marketing teams who are furious at having their customer growth figures threatened. Unfortunately, while security teams are facing pushback from all sides, it's these hurdles that protect the business. In order to ensure that organisations are protecting their users without driving them away, it is essential to understand when and where to place these hurdles.

## The balancing act

In order to implement an authentication strategy that doesn't drive away customers, businesses need to make customers experience the focal point. If an organisation can adaptively adjust their authentication solutions based on user context, they can intervene appropriately when needed. This starts with lifting the burden of authentication off of users and focusing more on device authentication. If an organisation can effectively authenticate a user based on the device they are using to sign-in, then that user doesn't need to be troubled with MFA until they start making changes to personal details or making large transactions that might warrant an additional layer of security.

This risk-based approach to authentication is ideal as customers are more accepting of friction where they perceive a greater risk and if a business is seen to be protecting what is most valuable to the customer, the friction is not only accepted, but appreciated. But how do we determine where a user's tolerance for security lies? Whether or not it's regulated should be a good indication of how much security it needs! But for the data that doesn't fall into these categories, canvassing your users and customers is a good way to get a feel for the general level of tolerance.

Customers should be provided with transparent access and control of their security, such as what permissions they have and their trusted devices. By doing this, organisations empower their customers to manage their own digital security. Help them establish habits, regularly remind them to check their security and trusted devices. These alerts should be easily dismissible but bring the ideas of security to the forefront and reminds customers they have the responsibility for their identity and security.



*“Security teams have to bring all the stakeholders together and make them a part of any decision”*

## Security vs the world

It can be hard for security teams to get the right authentication solutions in place when they are battling with the business as well their users. Statistics show that even minor amounts of friction can have a big impact on customer behaviour, so it's understandable that business leaders and marketing teams want to ensure that their customers are impacted as little as possible. A simple solution to this is to get security involved with marketing in the early stages to discuss the customer journey and to work together to find a solution that offers a balance of friction and ease of use.

For the many that are already past the early stages, our panel of security experts saw success when they brought the business stakeholders into their tabletop exercises. When the wider business is made aware of the realities and risks of data breaches, the discussion changes from "why do I have to do this?" to "how do we do this in a way that works for everyone?"

## Building user confidence

The value of authentication is most commonly understood about in terms of prevention. Even the most stubborn board members will look up when they are told that publicly traded organisations who have suffered a security breach see big share price losses and hits to long term customer growth. Not only that, but the group of customers that place a high value on security is growing every day.

Newer generations are more tech savvy and more likely to accept the necessities of security as well as walk away if they don't trust a business with their data. Even when users find authentication aggravating, they by and large appreciate the extra consideration of their security, and by providing the additional value to those who care about privacy and security, organisations can increase their acquisitions of this growing demographic.

Security is seen as a cost centre, but when you do customer authentication right, it drives revenue. Effective customer authentication builds brand loyalty, trust, and moves the needle forwards in terms of revenue. Security is quickly becoming linked to business revenue metrics in a major way and the importance of building trust and customer loyalty for growth and retention cannot be overstated.

## Getting it right

Customer authentication is an essential step for the modern business. While friction is a major concern, but technology exists to shift the burden of security onto technology for smarter, more risk-based security solutions. But even where friction is unavoidable, customers have repeatedly shown that they are more than happy to embrace friction where it is necessary and where it is clearly explained.

Deciding what authentication strategy works best is not a decision to be made in a vacuum and it doesn't happen within security teams alone. Security teams have to be willing to bring all the business stakeholders together and make them a part of the decision as well, even if that means having them shut down an idea as both sides work towards a compromise that serves everyone's business goals.

Battling the status quo to implement effective security is never easy, but there is a general trend towards consumers and businesses both wanting to do better with security. By working towards educating your customers on security and empowering them to take responsibility for it, businesses can move away from the concerns of friction and instead focus on leveraging technology to improve the customer experience. At the end of the day, the value of authentication can't be ignored. Yes, it will protect your business from cyber-attacks, but when done right, will allow you to create customer experiences build trust and drive growth beyond your competitors.

Rela8 Group serves the technology leaders community by giving executives a platform to identify challenges, connect with key innovators and understand where their business is going next. Based on these three pillars, we create engaging and stimulating B2B programs as well as custom gatherings for senior leaders and solution providers.

technology **leaders club**

rela8 group