BEYOND IDENTITY

What brands get wrong about customer authentication

WHITEPAPER | FEBRUARY 2022

technology leaders club

Because it serves as a product gateway, customer authentication is a critical component of almost every app that exists, impacting 100% of customers.

It is not easy to get right, and the stakes for getting it right are higher than ever with 46% of customers abandoning a transaction because of authentication and account takeover fraud increasing by 29% in 2020.

We hosted a roundtable that brought together security architects, IT, network & security operations directors, process & innovation professionals to take a deeper look at:

- What frustrates customers the most about app authentication
- How to balance friction versus security when evaluating customer authentication solutions, such as MFA
- Why reducing fraud and account takeover builds long-term customer retention

> 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 fundamentally changing the way the world logs in – eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication. Their invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements and improve the user experience and conversion rates.

Their revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device and continuously analyses hundreds of risk signals for risk-based authentication.

Customer authentication

Customer authentication is the cornerstone of our digital experience. There are so many things for organisations to consider including customer experience, engineering security and privacy. Unlike protecting employees, customer authentication is not just about mitigating risk. It also functions as a meaningful driver of revenue by decreasing friction and increasing security. Organisations need to ensure that their infrastructure is scalable, leading to better business outcomes.

Authentication and customer frustrations

Top of the list of customer frustrations is the sheer number of passwords they have to remember for different modes of verification on different platforms and/or devices. Being able to remove that friction and improve the customer experience is paramount.

Even creating an account can be frustrating because every company has different requirements. Consumers are advised to use password managers, but they cannot copy and paste passwords, and accessing a password manager adds another level of frustration. Organisations are therefore creating barriers to entry that can cause high drop-out rates. Therefore, there has to be a balance between having security and operating the business.

There is a difference in risk between logging on to a bank and a social media platform. For financial organisations, there is a lot of friction from customers regarding password requirements but additionally there are regulatory and legal/compliance pressures to increase security by adding more steps.

So, the password path seems to be unsustainable from both a customer and a security perspective. One of the key drivers for modern authentication is therefore to shift the burden away from users and put the onus on proven technology. Modern cryptography can resolve the complexity of centralised certificate management, so perhaps a similar schema could be deployed to eliminate password use. Although the implementation of a better solution would have to satisfy regulatory and privacy requirements.

Friction vs security

Historically, identity authentication and security have not necessarily been developed together at the same time. Organisations may have a team for each with conflicting priorities because increasing security increases friction. Companies should address these issues collectively, developing solutions together so things are more streamlined. However, there is no one size fits all and every company has to determine the balance point between friction and security individually.

But does friction and security always need to be a balancing act? In risk-based authentication, the focus has shifted to using friction as a strategic lever that can be deployed when the risk levels are appropriate, based on specific tolerance. For example, when a large financial transfer takes place, or the user is in a different geographical location or they log on at an unusual time, the trusted authentication method is requested again.

Username and password are not secure enough, especially as many people use the same ones for different companies. Another way of balancing security and friction is to implement multifactor authentication (MFA), such as username + password + text, biometrics + password, password and push notifications. All add an extra level of security. Consumers need to be aware that if downloading an app to help them with MFA, like any app download it could be malware, so should be checked out thoroughly.

> “
>
> The password path seems to be unsustainable from both a customer and a security perspective

Reducing fraud and account takeover

Customers may drive for less friction, but the drive for more security will always come from organisations and they will have to provide that part of the product. The customer expects that the organisation will have taken care of all this and any pressure on companies will come from regulators and/or legislation.

If there is a breach of security in a bank, then customers of other banks will ask their own bank what they are doing to protect them. They seek reassurance from the bank. This example demonstrates that although people care about identity theft, when logging on to a platform they assume that the company has taken this into account.

So, companies have to take the lead in security authentication and authorisation on behalf of their customers. Decentralised identity may be able to help to secure accounts so there is a reduction in account takeover and less fraud. Regulatory requirements for MFA may be outdated or not fit for purpose in today's environment when fraudsters know more about their target than the actual person does. Nothing will change until product, security and identity professionals think outside the box and all work together on a solution.

“

> Every company has to determine the balance point between friction and security individually

A balancing act

There is a fine balance between having a good level of security and operating a business. Customers become frustrated at the number of hoops they have to jump through to log on to a platform or application, and the password route seems to have become unsustainable.

One way forward is to look at the relationship between security and authentication and start developing solution for them both together, not looking at them in isolation from one another. Many organisations add an extra level of security by implementing MFA.

Even though consumers care about identity theft, they look towards organisations to take care of security for them. Taking authentication to the next level requires outside the box thinking with product, security and identity teams all working together towards one solution.

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