BEYOND IDENTITY

What Brands Get Wrong About Customer Authentication

WHITEPAPER | JUNE 2022

technology leaders club

Because customer authentication serves as a product gateway and impacts every customer, it is a critical component of virtually every app that exists.

It is important to get it right, but clearly not easy to do so with 46% of customers abandoning transactions because of having to complete authentication procedures. In addition, account takeover fraud increased by 292% during 2020.

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

- What frustrates customers the most about app authentication
- How to balance friction vs security when evaluating customer authentication solutions, for example MFA
- How reducing fraud and account takeover can build 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 the first and only company to provide passwordless identity management. The Beyond Identity team comprises cybersecurity and identity management professionals who are passionate about restoring digital trust and building a fundamentally secure way to authenticate and authorise users, whilst at the same time protecting the privacy of the individual.

Customer authentication

Are security and the user experience incompatible? Customers won't tolerate a bad user experience, so authentication has to offer the necessary level of protection to be safe from ransomware or credential-based attacks, but without making the customer experience too complex. The simple fact is that if a password exists on multiple servers - no matter how complex - it can be hacked, stolen, phished and used by bad actors for whatever purpose.

Password frustrations

Customers without photographic memories will find it impossible to keep up with the number of accounts and password formats required across multiple accounts and devices. Consumers are not interested in their own due diligence; they want to buy a product and they believe that the burden of security in the process lies with the vendor who is selling it.

For organisations with M&A (Merger and Acquisition) activities this can be particularly challenging as organisations may have to deal with disparate platforms and accounts. This is also frustrating for customers who may have to change their account set-up when a new company takes over. Providing a seamless transition for customers is challenging for engineers.

And not all MFA's are equal. Within the healthcare sector there are particular challenges for certain end-users who might struggle with technology, such as the elderly or those with impairments. Hospitals are also slow to implement new technology, and applying good security practices whilst running the day to day services of a busy hospital can be very challenging. Partners may not use best standards or duo accounts restricted to a single mobile device. It is difficult to know how to balance a requirement for MFA and a passwordless future in this instance.

The health industry in particular may always have to deal with the lowest common denominator from an end user perspective. Passwords have become a burden, holding everyone back from moving towards MFA or a passwordless future.

Friction vs security

When looking at a risk-based approach comparing friction for customers and security needs, one of the main challenges is to convince the generating revenue side of a business of the need for best practice from a security standpoint. Cybersecurity teams have to demonstrate the risks created by not putting measures in place - i.e. fraud, account takeover, etc - against the loss of revenue and abandonment of transactions on the other side.

One could highlight the differentiation or competitive advantages security measures could offer, and if authentication friction is reduced then fewer orders would be abandoned. The company may also gain new customers as the process to open an account and place an order is simplified. Educating sales leaders on why friction vs security is a problem, how it can be addressed, and which strategies can be used to move forward, is key.

There are costs associated with some risk based systems, but comparing the costs associated with fraud to those of implementing new security measures will likely justify the purchase.

> "If authentication friction is reduced, orders are abandoned less frequently"

Competitive advantage

Cybersecurity breaches are not just expensive in monetary terms. They make headlines which can be extremely damaging reputationally, especially if the breach may have affected thousands of customers. The damage from a cybersecurity breach to a company's reputation and future sales, as well as its stock value, could be far greater than the upfront cost of investing in more effective security. Once trust in a business has been broken it can take many years to rebuild. In the meantime, customers may move their business over to companies whom they perceive will better protect their data.

Budgets naturally have an impact on choices around implementing security solutions as not all organisations have infinite resources. When choosing from risk based authentication methods, an organisation will need to pick the most effective system that their budget allows.

Some of the burden of security can be taken away from customers by using device based authentication, linking the geographical location and timings of log-ons to a particular identity, and utilising device biometrics, etc, making logging on to their account simple and hassle-free and, by doing so, encouraging repeat business.

Striking a balance

Consumers want a frictionless customer experience when using online accounts. They will often reuse or simplify passwords because they cannot remember multiple passwords for multiple accounts, which can leave them exposed to potential security threats.

It can be a challenge to talk about friction vs security with executives, but weighing the costs of potential future security breaches with the upfront costs of updating security is helpful.

The cost of a security breach to an organisation is not just the fraud itself, but the damage to its reputation and future sales. Therefore, implementing robust security measures that do not increase friction for customers can give an organisation an advantage over its 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