TMT ANALYSIS

A COMPLETE GUIDE: STRENGTHENING AUTHENTICATION USING A MOBILE NUMBER

TMTANALYSIS

www.TMTanalysis.com

In recent years, the need for strong authentication methods has become increasingly vital as online threats continue to evolve. One such method that has gained prominence is mobile number authentication. By leveraging mobile numbers, businesses and platforms can enhance the security of their authentication processes and provide users with a safer and more streamlined experience when using their business applications online.

The Importance of Secure Identity Verification

Identity verification lies at the heart of maintaining trust and security in the digital world. With the growing number of identity thefts and data breaches, businesses and individuals are becoming more cautious about granting access to sensitive information, particularly when stored online.

This is where mobile number intelligence can be utilised to strengthen identity verification by checking the mobile number and device are associated with the correct person. Creating a reliable and efficient way to verify identities and reducing the risks associated with fraudulent activities. Using our authentication product we can also provide reliable and secure methods for authenticating users when they are accessing online accounts, reducing friction and enhancing Strong Customer Authentication.

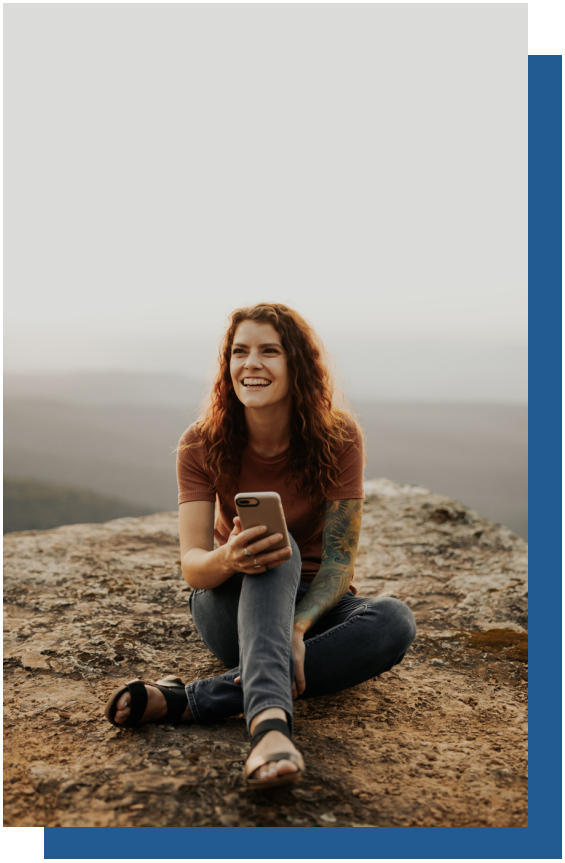
When pairing verification and authentication businesses can create robust security measures as they can tie the phone to the person, their device and the session.

What is Strong Customer Authentication (SCA)?

Strong Customer Authentication (SCA) is a regulatory requirement introduced by the European Union to enhance the security of online transactions. It mandates the use of two or more independent factors to verify the identity of the user. Mobile numbers are a convenient and secure factor that can be easily incorporated into the authentication process, ensuring one level of compliance with SCA guidelines.

The Role of Mobile Numbers in Modern Authentication

Mobile numbers provide a unique and reliable identifier for individuals, simplifying the authentication process for both businesses and users. By reducing the reliance on complex usernames and passwords, mobile number authentication reduces the likelihood of forgotten credentials, password reuse, and other security vulnerabilities.



Mobile numbers go beyond their traditional role as communication tools and have emerged as a fundamental component of modern authentication methods. Given both their widespread use and the fact that mobile is becoming the pre-eminent channel used by many businesses to interact with their customers, mobile numbers serve as powerful identification tools that can be leveraged to authenticate individuals across various platforms and use cases.

Leveraging Mobile Numbers as Identification Tools

Incorporating mobile numbers as identification tools creates a seamless and user-friendly authentication experience. By associating a mobile number with a specific user account, businesses can verify the ownership of the number and ensure that only authorised individuals gain access.

93%

of people have a mobile phone number

Furthermore, companies who bind specific mobile numbers to accounts can significantly reduce instances of fraud where fraudsters or ‘bots’ attempt to open multiple accounts with the same number. Clearly the fraudster’s business model for using AI-powered bots diminishes if a different mobile number (that is verified) is required for each.

TMT Analysis Silent Authentication Process

As part of our authentication process, we use trusted mobile data from our extensive network of global providers. All countries are mandated to store accurate mobile number data, whether this is through the mobile network operators who are active in the country or a centralised governing body, which stores this information.

These checks are carried out in real-time and entirely in the background during the log-in process, without adding any additional friction and making it more cumbersome for a user to access their account online. This frictionless approach is known as 'Silent Authentication'.

When a user logs into an application utilising Authenticate, our fully secure optimisation process takes place in the background. This includes:

Step One - At the start of the customer journey, the user logs in online or selects your app and provides the mobile number linked to their account.

Step Two - The device is given a unique URL to call and is temporarily re-directed to the mobile network to authenticate it against the mobile customer account within seconds.

Step Three - The device identity is authenticated and the result is passed back to TMT Analysis out-of-band by the mobile network operator so that it cannot be intercepted/copied.

Step Four - Once authenticated, the customer continues within your website or app, creating a frictionless customer journey.

How Mobile Numbers Enhance the Authentication Process

Mobile numbers enhance the authentication process through their ability to provide real-time verification and instant communication. By sending verification codes and links via SMS, businesses can instantly confirm the identity of the device, reducing the risk of unauthorised access.

The authentication process is enhanced because it allows the brands to have a definitive link between the device and the customer, and gives the customer satisfaction that the brand is taking account security seriously.

Two-factor Authentication (2FA) with Mobile Numbers

Two-factor authentication adds an extra layer of security to the authentication process by requiring users to provide two independent forms of identification. Mobile numbers serve as one of the most widely used and reliable factors for 2FA, significantly strengthening the security of user accounts and allowing organisations to comply with SCA guidelines as discussed above.

Adding an Extra Layer of Security with 2FA

By incorporating 2FA with mobile numbers, businesses can ensure that even if a user's password or other primary credentials are compromised, unauthorised access becomes significantly more difficult. This extra layer of security helps protect sensitive information and safeguards user accounts from malicious activities.

Utilising SMS Codes and Verification Links for 2FA

SMS codes and verification links sent to mobile numbers serve as an effective means of implementing 2FA. These codes are delivered directly to the user's mobile device, ensuring secure and convenient access to the verification process. By requiring users to input the code into the authentication interface, businesses can verify the possession of the mobile number and the legitimate user attempting to access the account.

Advantages of Mobile Number Authentication

Mobile number authentication offers several advantages over traditional authentication methods such as SMS. These include stronger security, increased user convenience, a more simplified user experience, and regulatory compliance with requirements like SCA. By leveraging mobile numbers, businesses can enhance their security and foster trust with their users.

Balancing Security with User Experience

While security is critical, it is essential to consider the overall user experience when implementing mobile number authentication. **Recent research has shown that 49% of all abandoned transactions are due to friction** and all businesses strive to strike a balance between security measures and user convenience, ensuring that the authentication process is smooth, efficient, and user-friendly.

It's worth pointing out that this adds friction to the user login process as your customer now faces additional steps and information to enter, in the form on an OTP (One-Time Passcode). Using TMT Authenticate allows you to carry out this process fully in the background, with zero impact on your customers.

Mobile Number Verification via SMS

Primarily due to its ubiquity (being available on all mobile devices) and ease of use, SMS One-Time Password (OTP) codes are by far the most common method of 2FA in use across the world today.

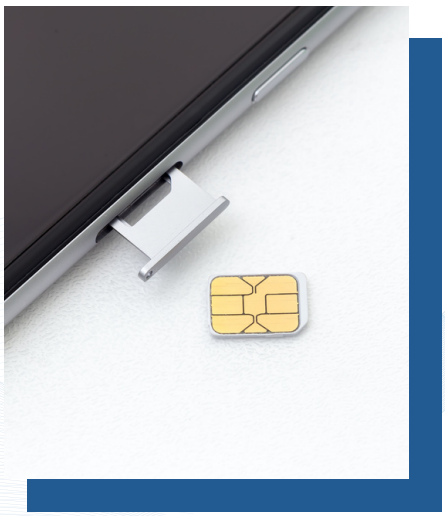
The Mechanics of SMS-based Verification

SMS-based verification typically involves sending an OTP as a text message to the user's mobile number. The user is then required to input the OTP into the authentication interface to complete the verification process.

OTPs delivered via SMS offer a unique and time-limited code for authentication purposes. These codes significantly strengthen security by ensuring that even if intercepted, they become useless after a short period. OTPs add an extra layer of protection to the authentication process, reducing the risk of unauthorised access.

The Danger of Sim-Swap and ATO

While mobile number authentication offers numerous benefits, it is essential to be aware of potential security threats. Although there are a number of different attack vectors that fraudsters seek to exploit, generically they are classified as Account Take Over (ATO) fraud. As the name suggests, ATO fraud involves the attacker taking control of a victim's device identity, following which it is possible for them to intercept all incoming calls and messages, including SMS OTP messages.



Security Challenges and How to Overcome Them

Despite the advantages of mobile number authentication, there are security challenges that need to be addressed. SIM swapping, identity theft, and social engineering attacks pose risks to the authentication process. Businesses should implement robust security measures, such as monitoring for suspicious activity, educating users about account security, and employing advanced fraud detection techniques.

Tackling Issues like SIM Swapping and Identity Theft

To mitigate the risks associated with SIM swapping and identity theft, businesses can adopt proactive strategies. These strategies include regularly monitoring for SIM changes, establishing strong identity verification processes, and educating users about the importance of securing their mobile devices and personal information.

Mitigating Risks and Ensuring Robust Authentication

Businesses must strike a balance between security and user experience when implementing mobile number authentication. By adopting industry best practices, utilising advanced security technologies, and keeping users informed, businesses can minimise the risks and offer a robust authentication process that protects both the user and your organisation.

Mobile Number Authentication in Various Use Cases

Strengthening E-commerce Transactions with Secure Verification

Mobile number authentication plays a crucial role in securing e-commerce transactions. By validating the identity of the user through their mobile number, which typically is the channel that they are using to interact with the user, businesses can protect against fraudulent activities and ensure a seamless and secure shopping experience for their customers.

Here are some ways mobile number authentication can enhance the security of e-commerce transactions:

1. Silent Authentication

By implementing silent authentication online stores can ensure the expected device is matched with the person when signing in and placing orders. This process works in the background and therefore adds no further friction whilst enhancing security measures.

2. Account Recovery

Mobile number authentication can also be utilised for account recovery in case of forgotten passwords or other account access issues. By linking a mobile number to a user's account, platforms can send account recovery codes or password reset links via SMS. This ensures that only the legitimate user with access to the registered mobile number can recover their account.

3. Fraud Prevention

Mobile number authentication can contribute to fraud prevention by detecting and blocking suspicious activities. By monitoring login attempts and transactional activities associated with a user's mobile number, platforms can identify and respond to fraudulent behaviour promptly. This proactive approach helps mitigate the risk of fraudulent transactions, protecting both the business and the user. Furthermore, organisations whose intelligent algorithms are specifically trained to highlight suspicious transactions can utilise mobile number authentication to check that a device has not changed and receive real-time actionable insights that can help prevent fraud in real time.

4. Compliance with Strong Customer Authentication (SCA)

E-commerce platforms operating within the European Union must comply with SCA regulations, which require two or more independent factors for user authentication. Mobile number authentication provides a convenient and secure factor to comply with these regulations, enhancing the security of e-commerce transactions and boosting consumer trust.

Reducing Fraud through Identity Verification

Mobile number authentication offers an effective means of reducing fraud across different industries, including online banking. By implementing robust identity verification processes that leverage mobile numbers, businesses can verify the authenticity of their users and prevent fraudulent activities that can lead to financial loss and reputational damage.

By exploring the topics mentioned above in further detail, businesses and individuals can gain a comprehensive understanding of how mobile number authentication can significantly strengthen the security of their authentication processes, while providing a streamlined and user-friendly experience.

Here are some ways mobile number authentication can help mitigate fraud through robust identity verification:

1. Know Your Customer (KYC) Compliance

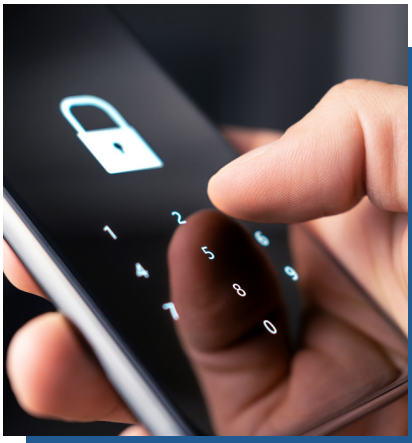
Many industries, including finance, healthcare, and cryptocurrency, are subject to regulations that require businesses to verify the identity of their customers. Mobile number authentication can be leveraged as part of a comprehensive KYC process to establish the authenticity of users. By associating a mobile number with an individual, and by verifying the number each time the user logs in, businesses can increase trust, deter fraudulent activities, and ensure compliance with regulatory frameworks.

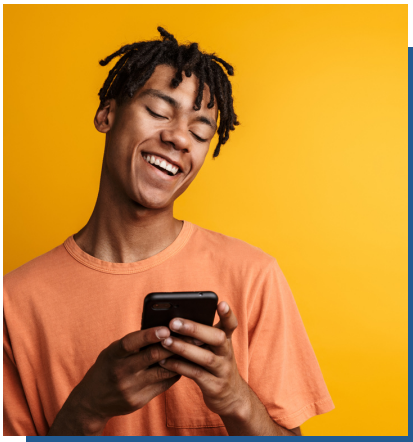
2. Anti-Fraud Measures

Mobile number authentication can strengthen anti-fraud measures by cross-referencing user information with mobile network operator data. This enables businesses to verify the ownership of the mobile number and detect potential discrepancies that may indicate fraudulent activities, such as account takeover or synthetic identity fraud.

3. Remote Identity Verification

In remote or online interactions, it can be challenging to establish the true identity of individuals. Mobile number verification provides a reliable and accessible method for remote identity verification. By requesting users to verify their mobile numbers through silent authentication, or a one-time password, businesses can ensure that the person accessing the account or service is the legitimate user associated with the registered mobile number.





4. Real-Time Verification

Real-time verification is a crucial aspect of identity verification to prevent fraudulent activities. Mobile number authentication enables instant verification by delivering authentication codes or links through SMS. The immediacy of this method ensures that fraudulent actors cannot gain unauthorised access to accounts or services, enhancing overall security and fraud prevention.

By utilising mobile number authentication, businesses can reduce fraudulent activities, safeguard user accounts, and protect sensitive information. The combination of identity verification measures and mobile number authentication offers a powerful solution to combat fraud across industries.

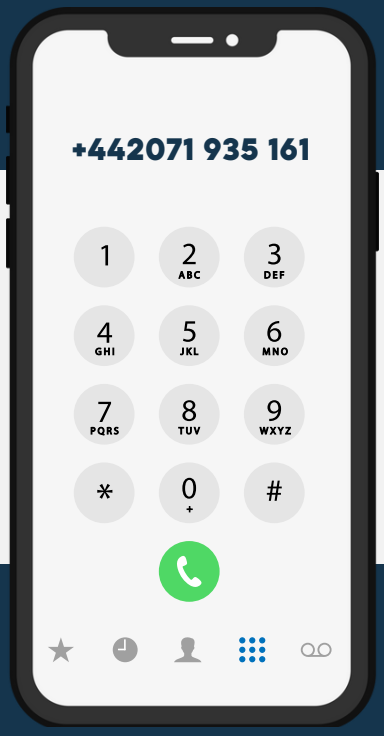
Conclusion

Mobile number authentication enhances security in the digital realm by utilising mobile numbers as a means of verification. By incorporating mobile number authentication or some other means of Strong Customer Authentication, businesses can strengthen their authentication processes and protect user accounts from unauthorised access.

While there are security challenges associated with mobile number authentication, ongoing improvements in technology and security protocols help overcome these obstacles. With its convenience, cost-effectiveness, and wide-reaching applications, mobile number authentication is becoming an increasingly important tool in safeguarding digital identities.

The latest offerings in mobile number authentication allow businesses to offer fully silent authentication services to their customers, providing top levels of security without adding any friction to the overall login process. If you'd like to know more about how this can help your business please don't hesitate to ask a member of our team.

WANT TO LEARN MORE?



Call us today to learn more about making your onboarding, authentication and verification process short, sweet and safe.

SCHEDULE A FREE CALL

Phone

+442071 935 161

Email

info@tmtanalysis.com