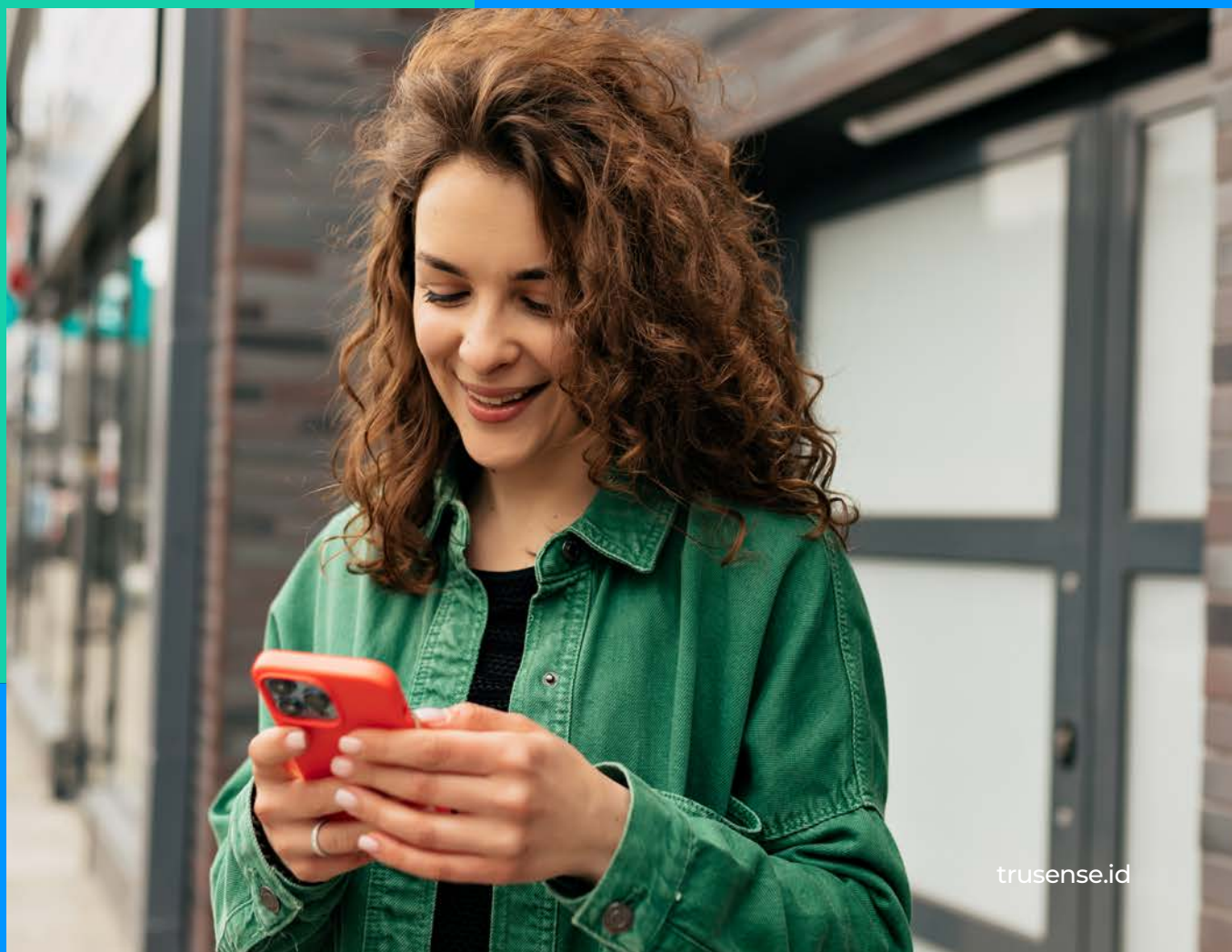
TruSense™

A Route Mobile Company

Time-tested Mobile Number Verification for better CX



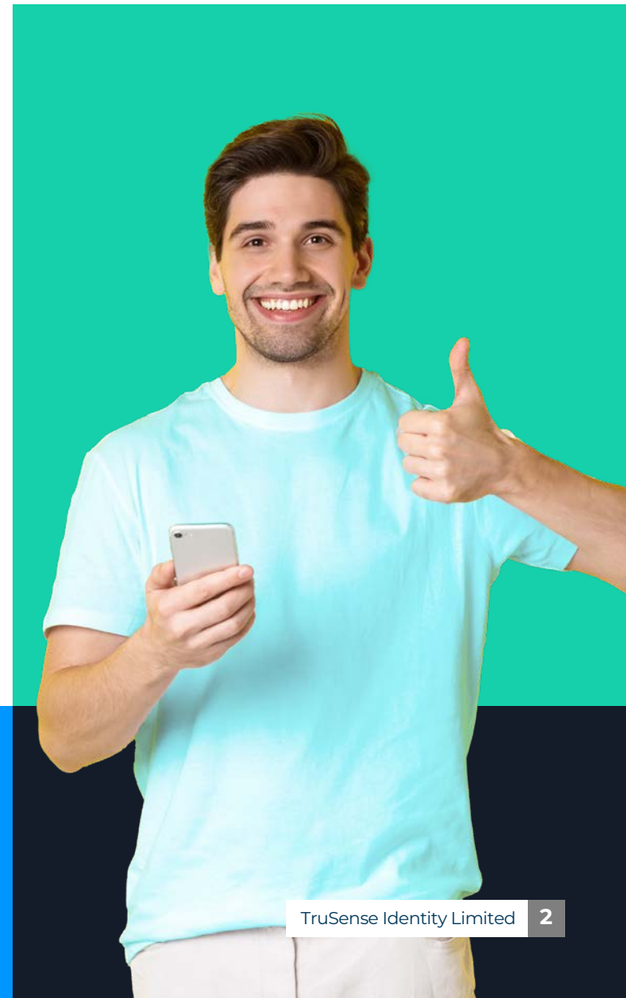
Index

Introduction

Human interaction and tangible physical documents, typically issued by central or local governments, have long been used to verify identity. Physical identification procedures, on the other hand, are no longer sufficient in today's society, where continual digitalization and 24/7 networking continue to disturb routine life.

In today’s world transactions are transitioning. And, with an increasingly connected culture users of online tools are familiar with the need for a user ID and password to access a variety of services. This requirement dates back to the early days of computers when systems demanded a digital means of user verification, and it has since been generalized to all virtual relationships.

Furthermore, customers are growing increasingly familiar with online banking, investing, bill paying, and even schooling as security-sensitive systems. Remote work access requirements are common among corporate IT users. It's become evident that reliable and powerful digital identity and verification schemes are required for the future growth of online companies. They will enable new players and organizations (public and private) to authenticate, identify, and operate effectively. This also includes safely using cutting-edge technologies like biometrics, blockchain, and artificial intelligence.



In October 2015[1], the GSMA revealed results from a research of 1,000 customers who answered the following question: ***"What documents or procedures do you plan to keep, or carry out, using your mobile phone by 2020?"*** The end results are listed in the table below.

Response	Consumers %	Response	Consumers %
Making a payment to an online store without cards	50	Storing loyalty cards and coupons	48
Tickets for travelling on public transport	35	Registering or sharing information with your doctor	35
Actively protecting yourself, your home and your family from hacking and fraud	33	Authorizing access to home Internet and TV	33
Storing your driving license	28	Proving your age when purchasing alcohol or cigarates at self-services check out	24
Filing your tax returns	23	Voting in elections	22
Entering your place of work, VPN, printers	19	Entering a country using a passport	17

The TSYS 2016[2] U.S. Consumer Payment Study asked 1,000 people to rank their interest in 14 different mobile services on a scale of one to five, with four being "somewhat interested" and five meaning "extremely interested." The percentage of respondents who expressed interest in managing various parts of their payments using their mobile devices is shown in the table below.

Service	Percent %
Immediately stop a transaction that was not made by you	69
Immedietely view transaction made with a debit or credit card	62
receive instant offers and promotions from the store you are visiting	54
Turn a payment card on or off based on location	53
Turn a payment card on or off based on type of store	50
Turn a payment card on or off based on time of the day	50
Keep all of your loyalty/reward cards on your phone	49

From the above surveys, it's clear that consumers are interested in increasing the quantity of data or managing payments and application credentials they retain on their smartphones.

Identity and verification is an essential aspect in the financial services industry. It's goal is to help businesses build trust between them and customers while maintaining the security of transactions. In regards to digitalisation, it is fair to say that the financial services industry is moving from an age of digital disruption to one of digital survival. This has happened for several reasons. Legacy players have been compelled to adjust as a result of digital-first banks. The appeal of entirely digital services has been fueled by challenger banks.

During the pandemic, the leading seven US challenger banks saw a 40%[3] increase in customer numbers, from 28 to 39 million. Legacy banks have been forced to rethink how they serve consumers to sustain market share and growth. Covid-19 has also contributed to the digital banking revolution. Digital channels, such as online and mobile, accounted for 82% of deposits in 2020. Furthermore, digital sales accounted for 42%[4] of overall sales. The adoption of omnichannel experiences is also on the rise; while 42% of Americans still open their primary checking account in a branch, 29% do it online. The remaining 30%[5] use more than one channel.

The younger, digitally native generation is fueling the transformation. Some customers will continue to favor non-digital options, but the trend is moving toward digital. Similar changes have occurred in the banking industry in the past. Online banking was formerly considered a novel notion. The majority of clients now make use of online services in some way. More than a quarter of millennials have never visited a physical branch, and approximately 40%[6] are considering going completely digital. Banks must at the very least provide digital as an alternative to appeal to the next generation of clients.

Also, non-bank firms who are expanding into the market are posing an increasing threat to banks. Fintech and payments companies that aren't bound by legacy infrastructure, for example, can more readily offer self-service, mobile, and 24/7 banking. This, in turn, encourages legacy players to embrace digitization and customer-centricity.

Lack of Traditional Verification Services in the Ecosystem

Customers expect their online journeys to be equally as secure, intuitive, and personal as their real ones, as digital and omnichannel experiences become more prevalent. To accomplish this, banks must improve their clients' identity and verification experiences. Customers are being let down by the way many firms handle identities. It's also obstructing their capacity to create trusting relationships with customers across the customer lifecycle.

Banks must execute identity verification (when a customer opens a new account) and customer authentication, according to regulatory requirements and best practices recommendations (when a customer further interacts with a bank, for example, high-risk transactions or account recovery). Identity checks were formerly conducted in person or through a database search. Usernames and passwords, KBAs, and call centers were frequently used for authentication.

However, in-person checks are getting less and less popular in today's world. They aren't scalable or convenient, but they are relatively secure. As stated earlier: nearly one-third of customers now open accounts online, and nearly a quarter of millennials have never visited a real branch. Customers' modern lifestyles are increasingly incompatible with branch-based banking because they're built on an all-or-nothing approach. Database checks, passwords, and KBAs fall short of security. Once hacked, they become obsolete and provide no future security for the customer.

1. http://www.gsma.com/personaldata/wp-content/uploads/2015/10/mc_us_paper3_10_15.pdf
2. https://www.tsys.com/news-innovation/resource-center/Research/research-paper-2016-us-consumer-payment-study.html
3. https://tradingplatforms.com/blog/2021/01/14/u-s-challenger-banks-record-40-user-growth-to-39-million-within-a-year/
4. https://www.finextra.com/newsarticle/37396/bofa-customers-go-digital-during-pandemic
5. https://myvelocity.com/resources/whitepapers/the-reacquisition-imperative/
6. https://www.fastinvest.com/en/blog/fintech-dilemma-customer-lifetime-value

Evolution of Mobile Verification Methods

As customers seek access to more platforms via their mobile devices, mechanisms for authenticating users on mobile devices have evolved, and while the speed of innovation is accelerating. This section discusses some of the most prevalent authentication systems used in the past, as well as their shortcomings, and some new mechanisms that are emerging to ensure that a user's identity is verified and validated in a fast, convenient, and secure manner.

01. User Id and Passwords:
A user ID and password are the traditional methods of authenticating users to an online service. On the other hand, the number of online accounts has grown to the point that the average American today has over 130 passwords. Both static and dynamic passwords are possible. The length, complexity, and timeout parameters are deployed because simple passwords are easily remembered.

However, such limitations can make entering passwords on mobile devices problematic. The primary shortcoming of passwords is the compromisation of security as they can easily be deciphered in today's world. Cybercriminal acts such as phishing can trick victims into sharing personal information. Even if new techniques are deployed to manage passwords, the development of new security and authentication methodologies offered by the power of mobile devices and related sensors promises to eliminate passwords in the future.

02. Multi-factor authentication:
Many digital service providers now use multi-factor authentication to ensure mobile ID authentication, because user ID and password strategies are becoming less popular.

Multi-factor authentication requires two or more of the following authentication factors:

- Documents such as driver's license, Aadhar Card, photo id proof, or tokens
- OTPs, numeric codes, or patterns
- Biometric characteristics, such as fingerprints, voice notes, or retina scans
- Location, or geofencing techniques
- Personal information, such as mobile phone numbers, or home addresses

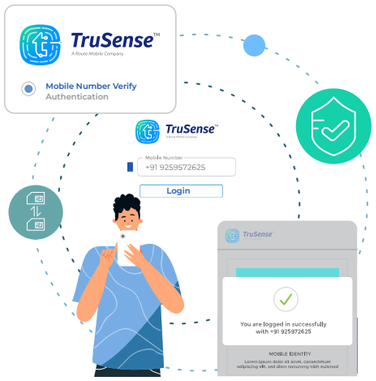
Although some of these methods outlined above come at the cost of CX, these methods add an extra layer of security and ease the process of mobile verification.

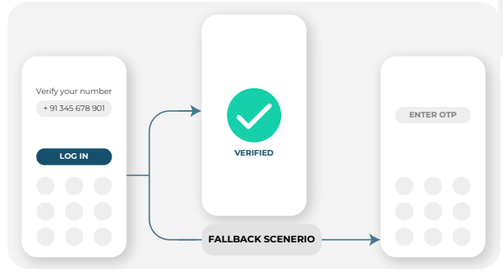
As an added note, it shouldn't be necessary to wait for a second code to confirm your password in a 2-factor authentication system. In fact, modern security should not require the usage of a username and password. It may seem difficult to prove your identity to apps and services without these necessities. However, security experts have long highlighted the system's flaws, and several methods of passwordless verification have been developed, verifying identity through more sophisticated methods that are far more difficult to deceive!

The common denominator among biometric, hardware and app-based solutions is that they all require the user to add extra steps to the authentication process, whether it's carrying around a device, fiddling with a QR code, or entrusting your biological identity to a server — all of which add friction and ultimately detract from an easy, streamlined user experience. What if we removed the idea of compromising user experience through user action, entirely from this equation? For doing this, we present **Mobile Number Verification.**

Mobile Number Verification

As an added security check, TruSense introduces a Mobile Number verification product that authenticates customers across frequent elements of the customer journey, such as registration and purchases. This reduces the possibility of fraudulent actions such as phishing and interception of One-Time-Passwords. Mobile Number Verification is completed in the background in milliseconds, causing no inconvenience to the customer experience. Hence we can see that Mobile Number Verification significantly reduces the involvement of the weakest link from the process- the User, by providing a swift, seamless and invisible background experience. It has notable features such as an extra layer of protection and an extra layer of convenience. Mobile Number Verification repurposes MNOs' very strong assets, namely the Subscriber Identity Module (SIM) and Network, which are ubiquitous, and MNOs conduct security enablement using the same core assets millions, if not billions, of times per day. It also ensures a consistent user experience and along with its seamless integration and easy-to-use API, it should be a go-to choice for customers.





Mobile phone numbers, in a sense, also have an implicit identity tied to themselves. They have an inherent value over other means of identity such as email ids. For example, there is no KYC check required to obtain an email id (generally), thereby generating an email id is very simple and someone can generate millions of email ids within minutes, whereas the phone number requires a KYC check in most geographies and is not as simple and straightforward to obtain. Therefore one can conclude there is an innate "Identity" behind the phone number.

Mobile Number Verification does not find its usage restricted for the purposes of Login/Authentication (which has commercial implications because Login is a one-time event these days, and services make it difficult for users to Logout, so using it for Login reduces the number of transactions). Mobile Number Verification is also useful in a variety of real-world situations needing to validate a device possession factor prior to online use cases such as making a payment, transferring funds, adding a new payee, changing personal account information, etc.

Mobile Number Verification can seamlessly fallback to OTP based verification in the event of fluctuations in data connectivity, network issues, etc., to ensure a seamless and smooth user experience.

Conclusion

Authentication of customers has never been easier but Mobile Number Verification ensures that it's done conveniently and with ease. Mobile Number Verification gives you the full power of security in real-time and delivers a superior CX for your customers. We know that the future is digital, and so is the digital identification procedure. So going forward our service will perfectly fit with the new generation of mobile technology and create a fully seamless service. It's a one-stop solution that integrates everything you need to capture, verify and authenticate your customer.

TruSense™

A Route Mobile Company

TruSense Identity Limited is a wholly owned subsidiary of Route Mobile Limited, a publicly listed and one of the leading CPaaS (Communication Platform as a Service) providers to enterprises, over-the-top players, and mobile operators. TruSense marks its initial presence in India, Colombia and Peru as part of global expansion.

At TruSense, we are focused on providing technology based solutions to a digitally connected world vulnerable to identity theft and social engineering threats. Our products enable seamless user identity verification, risk scoring to establish user trustworthiness and user authentication for all digital first organisations.

Deeply ingrained within enterprises and mobile operators, with our commitment to customer satisfaction, 20 years of experience in the Mobile Communication industry and our dedication to providing the best fraud detection system available, TruSense exists to help organisations achieve their goals.

4th Dimension, 3rd Floor, Mind Space,
Malad (West), Mumbai - 400 064, India

trusense.id