Instantly Confirm the Identity of Mobile Numbers for Financial Services, Healthcare and E-Commerce Transactions

Mobile Numbers are the De Facto Digital Identity

Mobile phone numbers are now the primary way that billions of people worldwide are identified when buying and selling online, opening accounts, verifying their age and authenticating themselves to contact centers. The increased use of mobile phone numbers as the preferred identifier means that banks, credit card companies, payment gateways, e-commerce providers, insurance companies, hospitals and other organizations should reassess how they obtain and use mission-critical information about each number, including:

- Line type mobile, wireline, VoIP and toll-free
- SIM tenure for mobile numbers
- Service provider ownership
- Porting history
- Status such as premium rate, unallocated and high risk
- Country of assignment

These types of insights enable customer service, marketing, risk management, fraud prevention and other departments to quickly and confidently verify a person's identity, detect possible phone scams and support business processes. These use cases also highlight how mobile phone numbers directly affect revenue, losses, brand reputation and customer satisfaction.

As reliance on mobile phone numbers grows, so does their attractiveness to fraudsters. In fact, nearly half of all fraud reported to the U.S. Federal Trade Commission starts with a text message or a phone call. These trends highlight the importance of partnering with a trusted source to protect both customers and the companies they do business with. Authoritative, up-to-date phone number data from a trusted source is critical for ensuring compliance with the Telephone Consumer Protection Act (TCPA), the Telecom Sales Rule (TSR), the INFORM Consumers Act and anti-money-laundering (AML) regulations.

How Mobile Phone Numbers Overcome the Limitations of Traditional Identifiers

Although traditional digital identifiers such as names, addresses, email addresses, IP addresses and biometrics will continue to play a role in fraud prevention and risk management, none of these are as dependable and consistent as the phone number on a global basis. Accurate phone number information provides businesses with additional insights that can overcome inherent drawbacks to other traditional identifiers.

For example, names and addresses are inconsistent due to character sets and abbreviations. Individuals and companies tend to have multiple email addresses, which can change frequently or be created on demand. IP addresses can be spoofed or masked via VPNs. The effectiveness of biometrics also varies geographically because many countries have different regulations and authorized uses. There is also the rapidly emerging risk of fraudsters using artificial intelligence (AI) and other technologies to impersonate legitimate users. Phone numbers provide a consistent way to authenticate users across countries despite such limitations and restrictions.

Instantly Confirm the Identity of Mobile Numbers for Financial Services, Healthcare and E-Commerce Transactions

Finally, each phone number is linked to a specific device via the IMSI/MSISDN. This makes it ideal for helping overcome common authentication problems such as outdated mailing addresses and P.O. boxes.

Digital Identity Intelligence Deployed Throughout the Entire Customer Lifecycle

Digital Identity platforms enable businesses to leverage global expertise and accommodate for the rise in using mobile phone numbers as the de facto digital identity signal. Industry-standard platforms enhance Know Your Customer (KYC) and Know Your Business (KYB) initiatives by instantly confirming the identity and trustworthiness of each user's mobile number for financial services, healthcare, insurance and e-commerce transactions.

The Financial Action Task Force's 2020 Guidance on Digital ID report says that when changes to customer information or transactions can be reacted to immediately, customers can be categorized into the correct risk ratings[1]. These insights enable organizations to allocate valuable resources to the right customers and help make more accurate assessments.

Authoritative, continually updated phone number information is also a must-have for regulatory compliance. One example is the INFORM Consumers Act, which requires online marketplaces to verify information about high-volume third-party sellers to identify and deter criminals from selling stolen, counterfeit or unsafe items[2]. By law, a phone number is one of the identifiers that marketplaces must collect, a robust digital identity solution can help marketplaces meet the law's requirement of verifying the seller's phone number within 10 days. In addition to ensuring regulatory compliance and avoiding expensive penalties, this verification helps the marketplace protect its brand reputation as a trusted place to buy and sell.

Block Account Takeovers Prevent Callback Fraud

By 2025, account takeover fraud losses will reach almost $17 billion globally, according to Juniper Research[3]. This type of fraud relies heavily on SIM swaps and port outs to hijack phone numbers and then use those to take over financial and other accounts. Victims do not realize that they have been hacked until they notice that their phone no longer has service, which they initially assume is a network issue.

Financial institutions and other authorized businesses can block account takeovers by using authoritative phone number data to instantly determine whether the person requesting changes is using a phone number that was recently ported. If it was, the risk is high, and now the business can use other data to investigate whether the person is a real customer or a fraudster.

Prevent Callback Fraud

Many businesses let people leave a callback number instead of staying on hold. Fraudsters exploit this option by leaving International Premium Rate Numbers (IPRNs), which look like standard 10-digit telephone numbers but incur steep charges when the business calls them back. Callback fraud losses run at least $1.82 billion annually, according to the Communications Fraud Control Association.

But simply blocking all callbacks to the country where the IPRN originated is not a viable solution because it also blocks legitimate customers from that country. Instead, businesses can use TruNumber Protect to automatically block calls to IPRNs and other known high-risk numbers and number ranges. Now legitimate customers still get the responsive service they expect and deserve, which is a positive experience that fosters sales and brand loyalty.

1. www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html
2. www.ftc.gov/business-guidance/resources/INFORMAct
3. www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-206-billion/

Find out how TNS can help you with a wide range of telecom solutions:

solutions@tnsi.com
tnsi.com

USA	+1 703 453 8300
Europe	+44 (0)114 292 0200
Asia Pacific	+61 2 9959 0800