Why mobile network operators are key to the success of a trusted digital identity

CONNECTIVITY

POSTED ON 07.17.20

The success of any digital identity framework is contingent on the trustworthiness of customer data. By leveraging their experience in managing and protecting customer data, mobile network operators (MNOs) have the potential to be major actors in the digital identity ecosystem.

Today, there are more than 5.1 billion individuals with a mobile subscription and 8 billion devices connected to mobile cellular networks[1]. By 2025, those figures will grow to 5.8 billion and 8.8 billion respectively[1], and nearly three quarters of internet users around the world will access the web solely via their smartphones.

Mobile connectivity is a powerful tool that is driving the digital transformation on a global scale. In addition to facilitating access to countless services including banking and insurance, eCommerce, and travel, mobile connectivity also has the power to offer **financial inclusion** to the unbanked and underbanked in developing economies.

However, simply having a mobile device is not enough. For people to perform all these essential daily tasks remotely from their phones, they must have a **trusted digital identity** in order to prove that they are who they say they are.

MNOs: major actors of the digital identity ecosystem

For any digital identity framework or ecosystem to succeed, it must be available and accessible to as many individuals as possible. MNOs have the ability to reach the vast majority of these individuals. With many of them boasting higher numbers of customers than even the BigTech companies, MNOs often span across borders to multiple countries or business lines. In fact, the top 30 MNOs in the world have well **over 6 billion subscribers combined**.

MNOs not only have access to a vast amount of data on their customers, but also to real-time device data and network information. According to a **study by Experian**, device identity intelligence can increase fraud detection by 45% over other systems. This includes device location data, roaming status, SIM lifecycle, billing status, and much more, all of which enable MNOs to detect suspicious behaviors and fraud.

With mobile devices playing an increasingly important role in our daily lives, they can be used to identify and differentiate legitimate customers from fraudsters. Thus, MNOs can leverage their data to reduce identity fraud and prevent account takeover not just for themselves, but also for relying parties such as banks or other service providers. A report from **Juniper Research** has found that **mobile digital identity**, which ensures identity verification through SIMs, will generate over $7 billion for MNOs in 2024. This is up from an expected $859 million in 2019: a growth of over 800%.

Fighting against identity fraud

Indeed, with the increasing use of digital files and the growing importance of digital data, breaches are now happening daily. In the first quarter of 2020 alone, 8.4 billion records have been exposed, a 273% increase compared to Q1 2019.[2].

Fraud also impacts the telecommunications industry. Subscription fraud, which includes identity theft and account takeover, is one of the fastest growing and most prevalent types of fraud facing MNOs today.

According to a recent CFCA (Communications Fraud Control Association) survey of MNOs worldwide, identity-related fraud accounted for US$29 billion in losses. This includes subscription fraud, account takeover, internal fraud, dealer fraud, social engineering, pre-paid equipment & services fraud[3].

Device fraud and theft is one major pain point for MNOs worldwide, especially since premium handset prices increase each year and MNOs are often the ones to subsidize the cost for their subscribers.

This strategy has been successful in attracting subscribers in the past and will undoubtedly be a key to growth with the launch of 5G networks and compatible devices. 5G handsets command a premium price and attract more lucrative subscribers. With significant investment being put towards 5G networks and handsets, MNOs need to minimize losses from identity fraud and device theft.

Identity fraud is not only detrimental to the telecommunications industry; it has also huge implications for other service providers, particularly financial institutions. Many banks and service providers rely on a customer's mobile phone as a method of verification. When logging into an account, customers are often asked to verify their identity through an OTP (one-time password) sent via SMS. However, following a fraudulent SIM swap, where a fraudster transfers a victim's phone number to a SIM in their possession, the fraudster can receive text messages with bank account authentication codes or payment transaction codes and manipulate customer's financial services.

According to LexisNexis, attacks on mobile financial services transactions are growing at a faster rate than the overall attack level. This growth is being driven by telecom account attacks and data compromises, posing a serious risk to the reputations of MNOs. In 2019, one MNO failed to have a lawsuit thrown out of court in which the complainant pursued the loss of millions of dollars in cryptocurrency allegedly caused by a SIM-swapping attack. This shows that MNOs may be liable in criminal scenarios in which cell phones are used as the primary attack vector.

Therefore, MNOs are facing increasing pressure to create **trusted digital identities** for their customers and to prevent fraudulent account takeover for their services and for customers of relying parties that use mobile devices for authentication.

Complying with KYC regulations and more

As the providers of communications infrastructure in every country, MNOs are obliged to protect their networks and verify who can access it. Furthermore, regulators across the globe are becoming increasingly involved in the telecom industry in their fight against terrorist attacks, money laundering, and other criminal activities. They thus require telecom companies to strengthen their **Know Your Customer (KYC) and customer ID verification** procedures as a means of combatting nefarious use of mobile devices and fraudulent identities to perpetrate crimes. More than 150 countries now require proper registration with a strict identity verification service for the purchase of a prepaid SIM, following recommendations from the GSMA.

In addition, as MNOs continue to expand their financial services offerings, they are required to comply with KYC, anti-money laundering (AML) regulations, and combatting the financing of terrorism (CFT) legislations, which vary depending on the country.

As the compliance demands increase, the manual process of onboarding customers and verifying their identity becomes more time-consuming, operationally demanding, expensive, inefficient, and unreliable.

Digital onboarding can help MNOs **overcome the KYC and ID verification challenge** by automating the identity verification process and layering multiple checks: ID document authentication, biometrics and liveness detection checks, AML/CTF database screening, as well as third-party database checks. Software algorithms are also better equipped to detect sophisticated types of fraud such as document fraud.

A move from a prolonged, paper-based and inconvenient process to an entirely digitalized onboarding journey is a true game changer. It simplifies access to services and meets the demands of today's telecom consumers, while reducing processing time and costs for MNOs. With optimized processes, MNOs can benefit from fewer branches to maintain, lower overheads, lower customer acquisition costs, and a higher degree of trust in their customers' identities.

According to **McKinsey**, digital identity-based onboarding processes have the potential to reduce onboarding costs by up to 90 percent.

Furthermore, by enhancing data accuracy and delivering a 360° view of the customer across the account lifecycle, digital identity systems enable MNOs to gain customer insights, create richer customer profiles and provide highly tailored customer experiences and offerings, boosting loyalty and building stronger relationships.

Digital identity to support MNOs diversification strategy

This enhanced digital identity can also support the diversification strategy of MNOs, which move into new businesses, such as finance, insurance, media, energy, healthcare and retail – all to increase revenues and profits in a highly competitive market. All these adjacent activities require **trusted digital identities**.

Moreover, MNOs are in a distinct position to offer identity services such as customer onboarding, fraud detection and authentication to relying third parties, to help them verify their customers' identities and fight against fraud.

Assuming the role of identity provider, MNOs can provide valuable transactional identities to their customers and the customers of companies in adjacent markets, enabling mobile users to benefit from their telecom digital ID in their daily use of online services.

Gaining an even stronger foothold in the mobile world

Digital identity is more than something MNOs must implement to fulfil regulatory requirements and fight against fraud. It represents a great business opportunity for them. Digital identity is the key for MNOs to become a central player within the digital ecosystem.

Much like how the mobile phone is a critical part of our daily lives today, so too is a trusted identity provider. As the digital transformation continues throughout every industry and identity becomes essential for all digital interactions, MNOs have the opportunity to become a trusted identity provider and climb up the value chain of digital services.

---

[1] The Mobile Economy 2020, GSMA Intelligence
[2] RiskBased Security, 2020 Q1 Report, Data Breach QuickView
[3] 2017 Global Fraud Loss Survey, Communications Fraud Control Association

---