Mobile network operators can win the fight against identity fraud

CONNECTIVITY
IDENTITY

POSTED ON 06.07.21

Consumers turn to online channels for every aspect of their life: work, entertainment, shopping, financial transactions, and interaction with others. And while these trends were already in motion pre-pandemic, social distancing and the resulting shift to online commerce have created new customer habits that increasingly depend on digital availability.

According to a recent study by McKinsey & Company[1], on average, digital offerings have leapfrogged seven years of progress in a matter of months. What's more, over 60% of those surveyed believe that this **shift in consumer behaviors** and demands is "most likely here to stay."

While these shifts represent an enormous opportunity for enterprises to reach customers in new and innovative ways, the increased dependencies on digital channels has also resulted in the rise of online identity fraud and theft. And in this battle, one surprising actor comes out as a major player in the fight against online fraud: mobile network operators (MNOs).

The global impacts of identity fraud

Global mobile adoption has naturally spurred the ubiquity of online experiences and thus the sharing of personal data. Unfortunately, one result of this has been the growing threat of identity theft or identity fraud. In fact, according to the GBG State of Digital Identity 2020 report[2], 1 in 5 European consumers was affected by identity fraud in 2020.

Today, **false identities** are used to subscribe to telecom offers, enabling fraudsters to operate telecom services such as TV, internet services, mobile banking, mobile money, virtual wallets, and other high-value services. In 2019, the CFCA (Communications Fraud Control Association) reported that mobile operators worldwide recorded $28.3 billion USD in fraud-related losses—an increase of 37% compared to 2017[3].

Despite the outlook, MNOs are actually in a unique position to take back control, and leverage their role as telecommunications provider to further protect their subscribers and their subscribers' data with digital identity technology.

The role of mobile network operators and the fight against identity fraud

Many countries have already identified MNOs as key players in the fight against identity fraud. In fact, as of January 2020, 155 countries have mandated the registration of SIMs. This mandate requires MNOs to capture and **verify the identities of their customers** before activating service and granting them access to the network. These verifications

enable operators to achieve a higher level of assurance that a customer is who they claim to be, and thus diminishes the risk of identity-related criminal activities such as money laundering or threats to national security.

As providers of telecommunications services, MNOs dispose of a large amount of data—including device data, roaming, SIM swapping, and location data—that can enable them to detect and trace fraudulent activity.

This type of data could be hugely beneficial to relying parties (such as banks, retailers, or other service providers), who rely on MNO data to identify and authenticate customers who are looking to access their services under the same credentials. In acting as a digital identity provider, MNOs assume a key role in the fight against identity fraud.

Digital Identity: a major opportunity for mobile network operators

For any digital identity framework or ecosystem to succeed, it must be available and accessible to as many individuals as possible. With many mobile network operators boasting higher numbers of customers than even the BigTech companies, they have a reach that spans across borders. They are thus uniquely positioned to reach a good part of the world's population.

Identity proofing solutions can help MNOs accelerate and further secure subscriber onboarding processes—providing a seamless and user-friendly experience to new customers. Asking customers to take a photo of an official ID document means that it can be analyzed and verified for its authenticity. Similarly, a selfie portrait taken on a smartphone enables an extract of a biometric template that then can be compared to the portrait of the ID document, or even against a trusted national database—depending on local regulations.

Using these digital identity solutions, MNOs can create fully digital onboarding journeys that enable them to verify and register their subscribers' identities—fulfilling KYC and AML regulations required by many countries, while reducing processing time and costs.
This save billions of dollars collectively.

Digital identity for a richer customer experience

While one of the primary role of digital identity is to fight against these identity fraud challenges, these solutions also augment an MNO's position in the identity ecosystem value chain as a provider of trusted identity services.

By enhancing data accuracy and delivering a 360° view of the customer across their lifecycle, digital identity systems enable telecom operators to gain customer insights, create **richer customer profiles**, and provide highly **tailored customer experiences**. In doing so, subscribers can use their registered identities to access key services such as banking, payment, eCommerce, health, and more.

With digital **identity proofing solutions**, operators can turn their regulatory obligations into opportunities that will enable them to fight against fraud, and save billions of dollars collectively— all while benefiting from **accelerated subscriber onboarding processes** and new revenue streams derived from digital identity services.

Despite the risks they're facing, MNOs already dispose of many of the defenses they need to fight against growing mobile fraud, including network access, traceability services, and, most importantly, subscriber trust. The addition of identity proofing and verification services would not only add additional defense against growing identity fraud; it would enable mobile operators to future-proof their own business and meet their subscribers' demand for more optimized digital experiences.

In today's highly competitive mobile market, this type of framework could be the differentiating factor that sets them apart from other players on the market.

---

[1] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-

has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
[2] GBG State of Digital Identity Report 2020 | Digital Identity (gbgplc.com)
[3] 2019 Global Fraud Loss Survey, Communications Fraud Control Association