WHITE PAPER

How mobile operators can use digital identity to fight identity and subscription fraud

Effective identity verification services are key to addressing telecom fraud, complying with regulations and protecting your brand reputation

IDEMIA

Contents

Subscription and identity fraud account for over 30% of the financial losses faced by mobile network operators[1].

[1]2017 CFCA (Communications Fraud Control Association) survey

1 Digital identity and mobile operators

Today, there are more than 5.1 billion individuals with a mobile subscription and 8 billion devices connected to mobile cellular networks[2]. By 2025, these figures are expected to grow to 5.8 billion and 8.8 billion respectively[3], and nearly three quarters of internet users around the world will access the web solely via their smartphones.

Mobile connectivity has been a powerful catalyst of much of the digital transformation taking place across the globe. In addition to facilitating access to countless services including banking, insurance, and eCommerce, mobile connectivity also has the power to bring financial inclusion to the unbanked and underbanked in developing economies. Today, 1.7 billion adults around the world remain unbanked, yet two-thirds of them own a mobile phone that could help them access financial services[3].

However, simply owning a mobile device is not enough to spur the adoption of mobile services. Before consumers will perform sensitive transactions, they need to trust that their mobile transactions will be protected against potential fraud and security risks. Juniper Research estimates that over half of the value of fraudulent remote payments in 2019 originated through mobile channels. They expect this figure to increase to over 70% by 2024[4].

Biometric methods embedded in mobile devices such as fingerprint recognition, face recognition, and voice recognition can help users create trusted digital identities that can be used to prove that they are who they claim to be when attempting to access a service. These identities provide both users and service providers with an added layer of security that helps protect against fraudulent activities.

[2]The Mobile Economy 2020, GSMA Intelligence
[3]The Mobile Economy 2020, GSMA Intelligence
[3]World Economic Forum
[4] Juniper Research, Online Payment Fraud, 2020

Mobile operators: key players in 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. With many mobile network operators (MNOs) 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.

As the providers of communications infrastructures, MNOs have a responsibility to protect their networks and to verify who can access them. Furthermore, as operators continue to expand their financial services offerings through mobile money services, they are being increasingly required to comply with Know Your Customer (KYC), Anti-Money Laundering (AML) regulations, and Combatting the Financing of Terrorism (CFT) legislations – each of which vary depending on the country.

''Mobile operators are uniquely positioned to drive the creation of digital identity systems and to unlock value for telecom and financial services and beyond.''

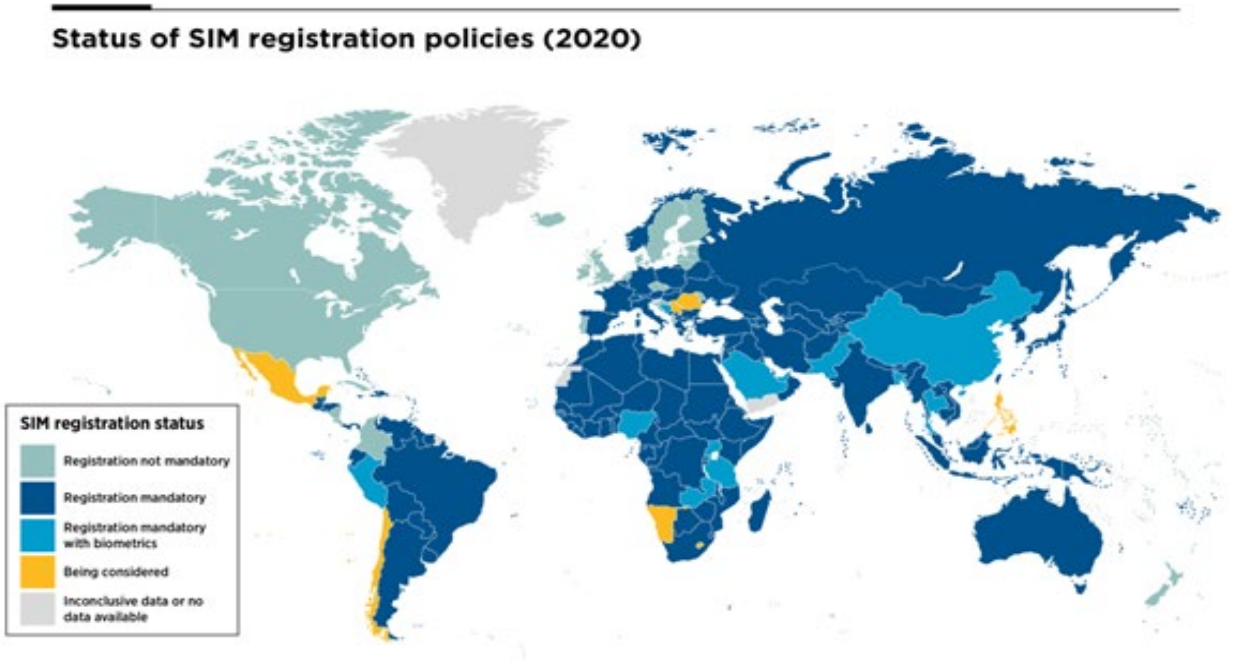
Maintaining compliance with KYC

As operators continue to extend their reach across the globe, regulators are paying a much closer attention to assuring that telecom operators are protected against terrorist attacks, money laundering, and other criminal activities. As a result, they are now requiring that telecom operators strengthen their KYC and customer ID verification procedures.

To meet these additional regulatory requirements, MNOs can connect their identity services to a System of Record (“SOR,” or sometimes known as a “Root of Trust”) such as a government database or department of motor vehicles, to cross-check demographic and biometric data (where accessible) and verify a customer's identity.

These verifications enable operators to achieve a higher level of assurance that a customer is who they claim to be. In doing so, MNOs not only meet their regulatory requirements, they also augment their position in the identity ecosystem value chain as a provider of trusted identity services to other relying parties. Following recommendations from the GSMA[5] , 155 countries now require proper registration with strict identity verification services for the purchase of prepaid SIM.

[5]https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf



Digital onboarding for an enhanced customer experience

A move from lengthy, paper-based process to an entirely digitalized onboarding journey is a true game changer. It simplifies access to the services and meets the demands of today's mobile subscribers, while reducing processing time and costs for operators. With optimized processes, operators can lower customer acquisition costs and get 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[6].

Furthermore, 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 and offerings, all while boosting customer loyalty and building stronger relationships.

[6]McKinsey Digital, Digital identification: A Key to Inclusive Growth, April 2019

2 Subscription and identity fraud

According to a 2019 CFCA (Communications Fraud Control Association) survey of mobile operators worldwide, fraud accounted for $28.3 Billion USD in losses, an increase of 37% compared to 2017[7]. This includes subscription fraud, account takeover, internal fraud, dealer fraud, social engineering, pre-paid equipment & services fraud, which are identity related fraud. Subscription fraud, which is a form of identity fraud, is one of the fastest growing and most prevalent types of fraud facing mobile network operators today.

FRAUD TYPE	DESCRIPTION
Subscription Fraud (Identity theft)	Use of a real identity without the owner's knowledge to obtain goods and services without intention to pay
Subscription Fraud (Fake identity)	Creation of false details to gain access to goods and services without intention to pay
Subscription Fraud (Credit Muling/ Proxy)	Use of real identity details (with authorisation for payment) to obtain goods and services, without intention to pay
Account Takeover	Manipulation and utilization of existing customer account in order to gain devices or service
Internal Fraud/Employee Theft	Theft of service or equipment by employees. Also includes abuse of company's credit and adjustment policy.
Dealer Fraud	All types of fraud conducted by indirect and third-party dealers
Social Engineering	Manipulation of an employee or customer to unintentionally give out important information
Pre-Paid Equipment & Services	Theft of personal information or credentials via hacking, phishing, vishing, etc. to get hold and acquire pre-paid equipment and services illegitimately

[7]2019 Global Fraud Loss Survey, Communications Fraud Control Association

Device fraud and post paid markets

It is interesting to note that as the price of premium smartphones continues to rise, so does the cost of device loss. This is especially true in North America and Western Europe, who offer different subsidy models for premium devices.

North America and Western Europe are two examples of "postpaid markets," a term which refers to markets where it's more common for subscribers to be on multi-year contracts that enable them to subsidize their phones.

In these postpaid markets, new customers are only obligated to provide a small down payment to receive a new handset.

A trusted digital identity would prevent fraudsters, who often capitalize on data breaches to sign up for new accounts using fabricated or stolen identity attributes and then make off with a new device.

Mobile money fraud

Mobile money services offer a popular alternative to cash, allowing users to store, send, and receive money as well as pay for goods using their mobile phone.

Widely used in regions such as Sub-Saharan Africa, South Asia, and East Asia, mobile money services enable consumers who are unbanked or underbanked to benefit from essential services such as mobile money transfers, benefit from mobile insurance, mobile savings and mobile credit services.

Mobile money has become a core product offering for many MNOs, who are increasingly leveraging their position to provide access to essential financial services. Today, there are over 1 billion mobile money accounts processing more than US $2 billion per day[8] globally. This represents a growth of 10% in registered accounts and 26% in transaction value worldwide, compared to 2017.

Despite the vast benefits, mobile money comes with risks of fraud, such as the potential theft of PIN or personal identification details, non-existent or ghost employees receiving funds, agents transferring funds to personal accounts, creation of accounts for false, invalid or duplicated customers, or manipulation in e-money reconciliation. Each of these contributes to high financial losses, both to customers as well as mobile money providers.

There have been several high-profile cases that highlighted the problem of fraud for mobile money providers. In 2012, a large mobile money provider in Uganda, lost an estimated US$3.5 million through internal fraud perpetrated by staff[9] . In a similar case in 2014, a provider in Rwanda was defrauded of US$700,000[10] in a sophisticated scheme conducted by an internal crime ring.

To protect themselves and mobile money users against fraud, MNOs can implement a trusted digital identity system for their customers (and agents) to secure sensitive interactions such as account opening, account access, SIM swapping, and more.

[8]State of the Industry Report on Mobile Money 2019, GSMA
[9]https://www.finextra.com/news/fullstory.aspx?newsitemid=23759
[10]https://www.newtimes.co.rw/section/read/183244

3 Digital identity for fraud prevention

The potential for subscription fraud exists at many different points along the customer journey. Fraudsters are targeting account opening, SIM registration, SIM swap and many other scenarios to try and gain access to subscriber accounts. Below, we look at each use case where a trusted digital identity can be implemented in order to prevent fraud.

Account opening and SIM registration

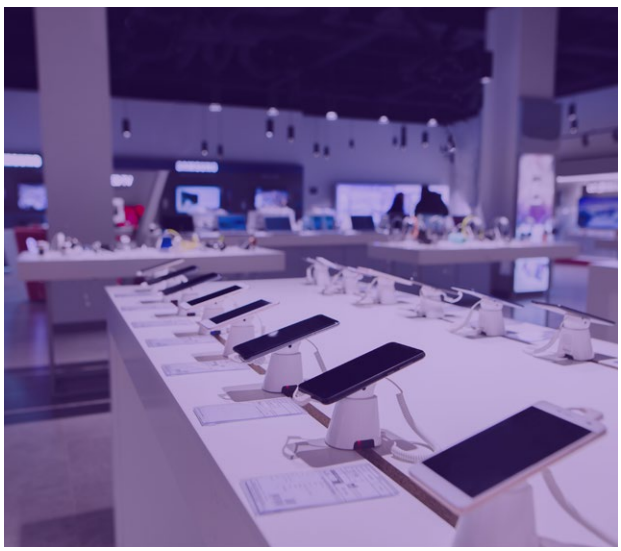
As of January 2020, 155 countries in the world mandate the registration of SIM cards[11] to reduce fraud, mitigate national security threats such as terrorism, and fight against money laundering and other criminal activities. This requires mobile operators to capture and verify the identities of their customers before activating service and granting them access to the network.

According to Reportlinker, the global market for SIM cards, estimated at 7.1 billion in the year 2020, is projected to reach 8.6 billion by 2027 - a CAGR of +2.8%[12].

As compliance demands increase, the process of manual onboarding customers and identity check is becoming more time-consuming, operationally demanding, expensive, inefficient, and unreliable.

Today, mobile operators can interact with their customers through an ever-growing variety of channels, including call centers, brick-and-mortar stores, web sites and mobile applications. Mobile and online channels are becoming more and more prominent and are driving new service transactions and online sales.

By incorporating identity verification as part of the account opening and SIM registration process, mobile operators can address a major source of subscription and identity fraud while also creating a seamless and consistent experience across all sales channels, throughout the customer lifecycle. This could enable them increase revenues, reduce costs, and boost their competitiveness.



[11]https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf
[12]Reportlinker - Global Subscriber Identity Module (SIM) Industry Report - September 2020

Watch list and biometric screening

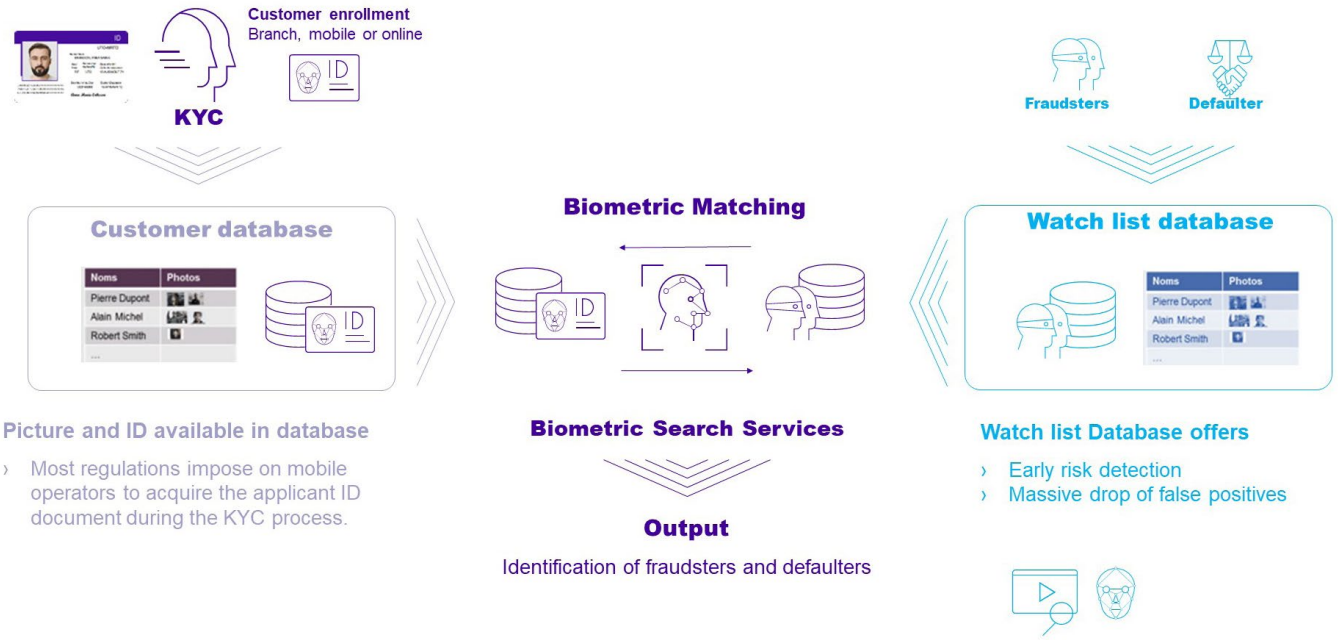
Typically, fraudsters will use stolen identities and go from store to store trying to open accounts and obtain devices for resale. To combat this, some MNOs create watch lists of fraudsters based on past incidents of fraud or theft – they rely on these watch lists to prevent fraudulent transactions before they occur.

However, a watch list containing Personal Personally Identifiable Information (PII) such as names, email addresses, date of birth, and credit card accounts, all linked to confirmed fraud incident, is not a complete solution, as fraudsters frequently use fabricated and stolen identities to commit further fraud.

As the use of digital files and online data storage continues to accelerate, so do data breaches. In the first quarter of 2020 alone, 8.4 billion records were exposed in the United States – a 273% increase compared to Q1 2019[13].

Biometric screening offers compelling advantages over alphanumerical databases not only to detect PII and identity theft, but also to spot misspellings, misidentification and data errors, fake ID documents using altered names or photos, as well as unidentified persons of interest.

The combination of static watch list verification with biometric screening, ID document validation, and root of trust database checks significantly enhances the ability to identify fraudsters despite the fact that they are using altered and, stolen identities.



[13]https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q1%20Data%20Breach%20QuickView%20Report.pdf?hsCtaTracking=5d936f78-de69-45a4-9ba5-03c2e9f20952%7C617588df-ee05-4a00-bbb1-191d6888f519

A look at the regulations impacting the use of biometrics

Governments across the world are implementing new regulations to protect consumer privacy and personal data security. These regulations define what falls within the scope of Personally Identifiable Information (PII), as well as what kind of information can be used to identify an individual. Traditional PII includes your name, date of birth, nationality, and other fixed attributes.

However, as technology continues to advance, the scope and definition of PII is rapidly evolving to include biometric information, such as fingerprints, facial images, and iris images. As a result, their use by public and private entities falls under the provisions of the privacy regulations.

Data privacy laws across the world

Today, more than 80 countries have adopted policies and rules aimed at protecting consumer data privacy, with many more considering proposals. Examples of new privacy measures include:

In Europe: the General Data Protection Regulation (GDPR) for European Member States specifically addresses biometric data. In effect since May 2018, GDPR includes requirements related to privacy impact assessments, privacy by design, enhanced consent requirements, new data subject rights, appointment of a data protection officer in certain circumstances, new obligations imposed on data processors, 72-hour breach notifications and new accountability requirements.

GDPR not only applies to organizations that are established in the 28 European countries; it also applies to non-EU established organizations that target or monitor EU data subjects. This makes GDPR a global law.

In the United States, there is no single, comprehensive federal law regulating the collection and use of biometric data. However, more and more states are addressing biometric privacy protection, including:

- Illinois: Illinois Biometric Information Privacy Act (BIPA)
- Texas: Texas Business & Commerce Code §503.001
- Washington: Revised Code of Washington (RCW) Annex §19.375.020
- California: California Consumer Privacy Act (CCPA)
- New York: Stop Hacks and Improve Electronic Data Security (SHIELD) Act
- Arkansas: Arkansas Code §4-110-103

In Canada: the Personal Information Protection and Electronic Documents Act, or PIPEDA, governs how private sector organizations collect, use, and disclose personal information in the course of commercial business.

In India: Aadhaar, the government's biometric identity system, allows for the usage of the Aadhaar number and biometrics for verification by private parties. The Indian Government has laid down a set of rules to ensure data security and privacy for the Aadhaar Project.

In the Philippines: the Data Privacy Act seeks to protect all forms of personal and sensitive information.

In South Korea: the Personal Information Protection Act is one of the world's strictest privacy regimes. Like the GDPR, it protects privacy rights from the perspective of the data subject and it applies to most organizations and even government entities.

In Japan: the Act on Protection of Personal Information (APPI) applies to business operators that hold the personal information of 5,000 or more individuals. Japan has other personal information protection laws that apply to the government and public organizations.

In Chile: Law No. 19,628 on Privacy Protection ("Data Privacy Act") regulates the treatment of personal information in public and private databases or bank registers.

In Nigeria: the Nigeria Data Protection Regulation (2019) mandates that all public and private organizations in Nigeria that control personal data are required to make their respective data protection policies available to the general public.

The legality of biometrics and fraud prevention

While the majority of these regulations protect the private data – including biometrics – of consumers, the processing of this data for the purpose of fraud prevention is explicitly addressed in some of these regulations.

As biometrics are considered a special category of data [GDPR's recital (47)[14]] biometrics may be used for the reason of public interest (for example, for fraud prevention purposes) or with the user's explicit consent, as stated in GDPR article 9.

Ultimately, it is the responsibility of organizations to properly assess their legal requirements when it comes to the capture, processing, and storage of PII and biometric data for fraud prevention.

[14]General Data Protection Regulation, Article 47

Insider fraud

It may come as a surprise, but insider fraud is one of the most prevalent threats faced by organizations today. Often more damaging than externally perpetrated crime, insider fraud can not only affect the financial health of a company, it can also result in serious damages to a company's confidentiality, data integrity, and overall reputation. Internal fraud and employee theft is one of the Top 10 fraud methods, in the telecommunications industry identified by the Communications Fraud Control Association[15]. In 2017 alone, the telecommunications industry lost a combined $1.47 billion[16] to insider fraud.

In the mobile network industry, there are various ways that insider fraud can be committed. For example, a salesperson could use a falsified identity to activate unqualified accounts, or to falsely enhance their sales performance. Another example would be using impersonation tactics to gain access to data and hardware and then sell them for profit.

Digital identity solutions can help mobile operators mitigate some of the risks associated with insider fraud. For example, the addition of a biometric capture – such as fingerprint or facial imagery – during employee onboarding, would equip organizations with an additional method to authenticate employees before providing them access to sensitive data or tools. With this strengthened authentication, accessing back-end systems or areas for inventory storage, and performing sensitive transactions such as signing new accounts, performing SIM swap or modifying customer information would be much more secure.

Account access and authentication

Account takeover is a significant problem for mobile operators, especially as mobile phones become increasingly used as an authentication factor. Today, a number of service providers – including banks, investment firms, and other enterprises – utilize SMS verification to authenticate their customers. If a customer loses their phone or account credentials, these accounts are at risk of also being compromised.

Mobile operators can leverage digital identities to secure customer accounts and apply multi-factor authentication depending on the level of risk associated with the access request.

For example, if a fraudster is attempting to gain access to a customer account using a new device or from a different location, the mobile operators can use these risk signals to perform a risk-based analysis and request biometric authentication – a selfie check for example – to assess the identity of the requestor.

This type of authentication can be applied not only to account access scenarios, but also to sensitive transactions, such as money transfer and payment.

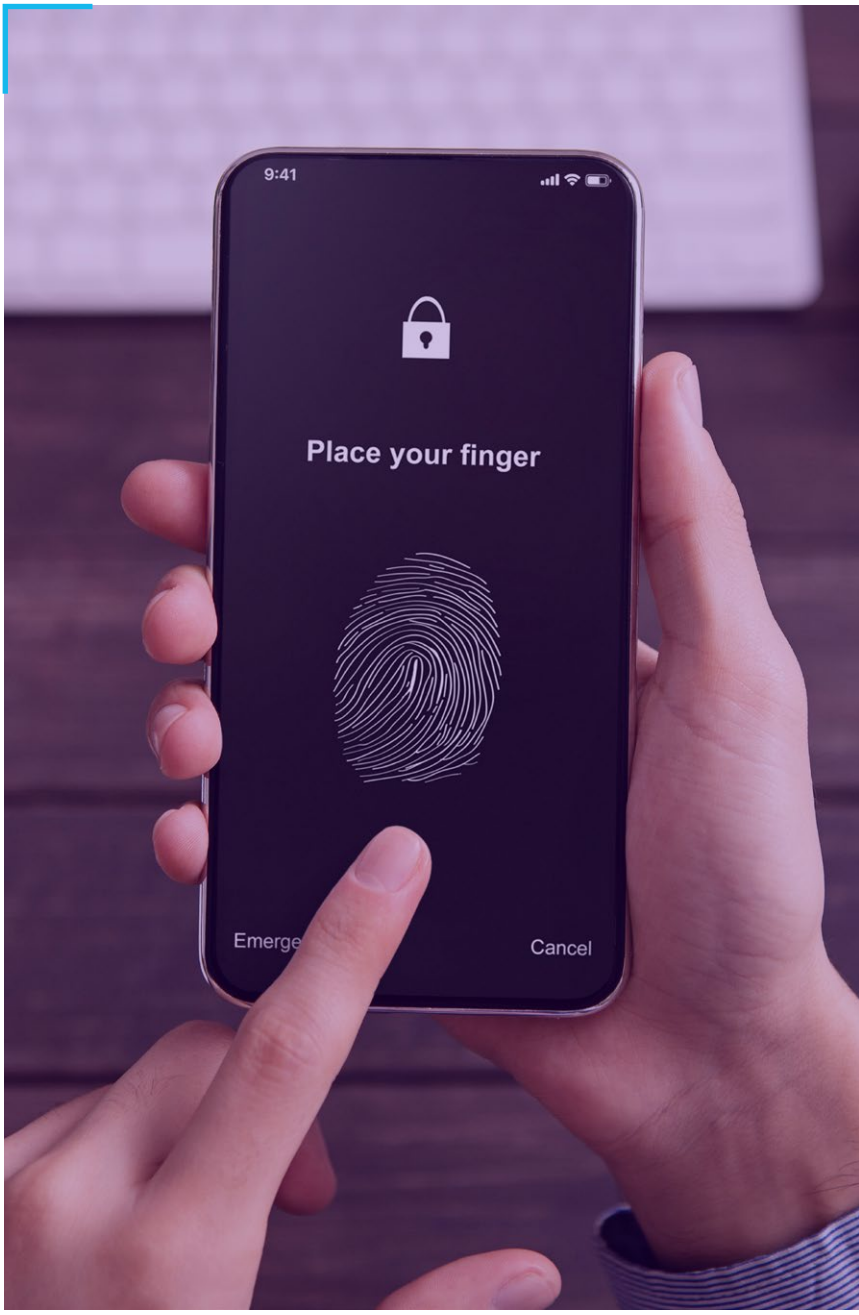
[15]2017 Global Fraud Loss Survey, Communications Fraud Control Association
[16]2017 Global Fraud Loss Survey, Communications Fraud Control Association

SIM swap fraud

Without strong multi-factor authentication, mobile operators increase the risk of identity theft and SIM swap fraud. Fraudsters use phishing and data breaches to obtain a victim's static credentials (name, date of birth, address, email) and assume the stolen identity to request a new SIM. They then have the line activated on their device and can make online purchases, passing SMS OTP (a temporary code that is automatically sent by SMS to the phone number) authentication without any problems.

This type of 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 SMS OTP as a method of verification. Following a fraudulent SIM swap the fraudster can receive text messages with bank account authentication codes or payment transaction codes and manipulate customer's financial services.

According to LexisNexis[17], 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 mobile operators.

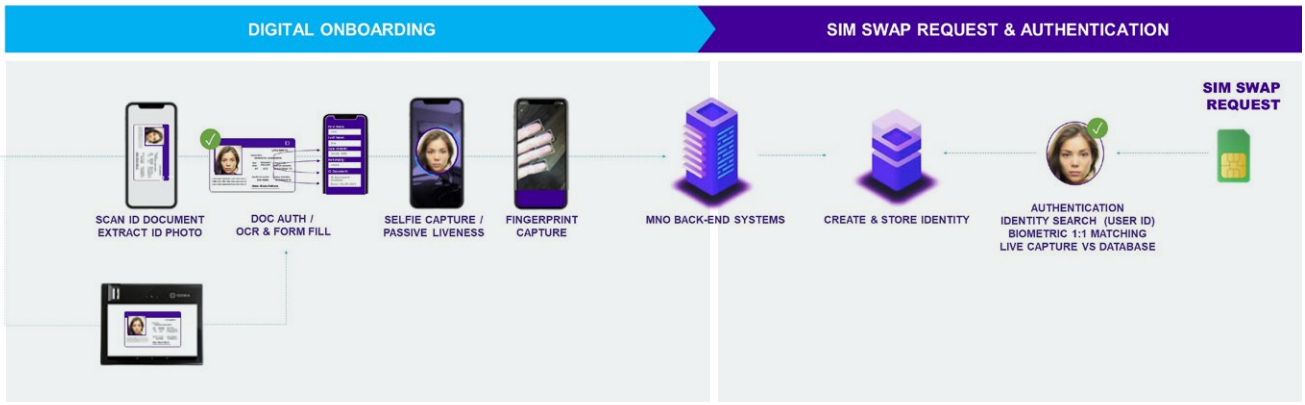


[17]https://risk.lexisnexis.com/insights-resources/research/the-q2-2018-cybercrime-report-from-threatmetrix

In July 2019, a large US-based operator failed to have a lawsuit thrown out of court in which the complainant pursued the loss of 24 million dollars in cryptocurrency allegedly caused by a SIM-swapping attack. This shows that mobile operators may be liable in criminal scenarios in which cell phones are used as the primary attack vector.

Requiring customers to create a digital identity during customer onboarding is a simple way for mobile operators to prevent SIM swap fraud. No matter the channel (in-store, call-center, website, mobile applications), the customer receives a notification with a link to access the authentication page where a live selfie is required. A liveness detection step adds a layer of security during the customer authentication since the fraudster will be blocked even if they present a picture, a mask or a video of the victim's face.

In addition to this, MNOs could work with banks and other relying parties to provide SIM swap status as one of many risk signals in transaction risk analysis. For example, if a bank receives a request to transfer a large sum of money, they could ask the mobile operator if the customer's SIM was recently swapped and, if so, they could then flag the transaction for further analysis.



4 Digital identiy beyond fraud prevention

MNOs as trusted identity providers

In a world where everything is connected, a trusted Identity Provider (IdP) acts as the ID provider for a relying party or partners and facilities trust between the various members of the ecosystem. The Identity Provider relies on their existing digital identifiers such as customer ID, and the need of reliable credentials such as biometrics, which they have already captured and verified.

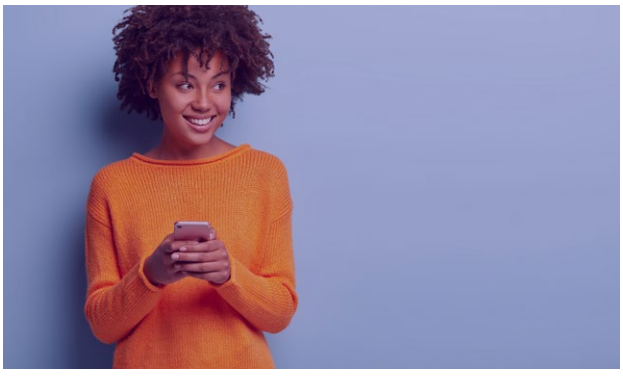
With a database of secure, verified identities, mobile operators would be in a strong position to become identity providers for third parties and their customers when they enroll or authenticate for those services. As identity providers, MNOs can provide valuable transactional identities to their customers 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.

A recent study by Juniper Research stated that mobile operators have a revenue opportunity of $7 billion from identity services alone.[18]

Mobile network operators are already more trusted by customers than social networks or other sources of identities. Using biometrics would add another level of security to their systems and give customer an even higher level of assurance.

Digital identity as a catalyst for diversification

An enhanced digital identity framework can also support the diversification strategy of mobile operators, enabling them to easily move into new sectors such as finance, insurance, media, energy, healthcare, and retail. This increased reach positions mobile operators to increase their revenues and their profits in a highly competitive market, by offering new services to their customers. MNOs are in distinct position to utilize identity services through specific use cases such as customer onboarding, fraud detection, secure access and transactions, enabling them to verify their customers and fight against fraud. By implementing digital identity in these use cases, MNOs can build on the same identity infrastructure to offer newservices to their customers.



By leveraging the created identity, mobile operators can enable a single sign-on experience for their customers, offering a seamless user experience for them, and thus enhancing their attractiveness and revenues.

[18]Juniper Research, Digital Identity: Technology Evolution, Regulatory Analysis & Forecasts 2019-2024

eSIM & eKYC

An eSIM, or embedded SIM, is similar to the physical SIM card except that there is no SIM card tray or removable component anymore. Instead, a digital profile is downloaded remotely from the mobile operator network and stored on the eUICC, or eSIM.

Since an eSIM is embedded in the device, it eliminates the need for customers to go to a store to activate a subscription. Now they can activate it anytime and anywhere – from the comfort of their own home or on-the go like when travelling abroad. Customers can browse different subscription plans directly on the device, complete the enrollment process, then instantly download the eSIM profile onto the device.

As more devices are connected with eSIM instead of traditional SIM cards, there will be an increase in demand for digital onboarding. Customers will expect to be able to activate and manage their subscriptions at any time without relying on customer service. eSIM technology is also creating a similar demand for other types of cellular-enabled devices such as smartwatches, other wearables, tablets, and PCs.

With 2 billion eSIM-enabled consumer devices expected by 2025[19], eSIM support can be a differentiator for mobile operators. By offering on-the-spot subscription activation for eSIM-enabled devices, mobile operators can not only attract new subscribers but retain them by adding more and more devices to each subscriber's bundle.

Combining digital identity verification technologies with eSIM devices means that MNOs will have the opportunity and means to create the completely digitalized onboarding journey that their subscribers expect, while simultaneously fulfilling KYC and AML regulations and significantly reducing fraud.

[19]ABI Research, eSIM in the Consumer and M2M Markets 2020

5 Identity verification solutions

A trusted and reliable digital identity requires a layered identity proofing approach. Mobile operators can choose which of the layered measures to take based on the profiles of their customers, their risk policy, and level of assurance requirements from local regulations. The identity verification proofing process helps to establish a level of trust with their customers that enables them to securely provide them with the appropriate products and services remotely.

The identity document verification process consists of capturing, extracting, and verifying data from an ID document. Depending on the use case, the capture of identity documents can be done using the user's smartphone, in a self-serve mode, or using a dedicated hardware in an assisted mode. Embedded security features and other characteristics (template, font, consistency between data...) are then detected, analyzed and verified to ensure the authenticity of the document.

Identity document verification

The identity document verification process consists of capturing, extracting, and verifying data from an ID document. Depending on the use case, the capture of identity documents can be done using the user's smartphone, in a self-serve mode, or using a dedicated hardware in an assisted mode. Embedded security features and other characteristics (template, font, consistency between data...) are then detected, analyzed and verified to ensure the authenticity of the document.

Biometric verification

A strong identity verification process may require a proof-of-life check to ensure that the person behind the device is both present and is the legitimate owner of the ID document – not a fraudster using a static image, wearing a mask, or presenting a pre-recorded video. This can easily be verified by conducting a facial recognition and liveness detection check, where a selfie of the customer is compared with the facial image printed on their ID document. Fingerprint and iris scans also provide a convenient and secure way of guaranteeing the uniqueness of a person's identity. Biometrics sensors can either be embedded in smartphones or in dedicated biometric devices.

Video KYC

Video KYC is a familiar and effective tool for mobile operators to conduct a live one-on-one conversation between a trained agent and a customer. During the call, agents can verify the identity of a customer through ID document and biometric capture and record the entire session for auditing and archiving. This process enables enhanced human interactions with video and live consultation, as well as enhanced identity verification combining automation and human expertise.

Mobile operators can use video conference to remotely verify the customer identity, to better engage with their customers, and to guide them through the onboarding process, while also complying with local AML and KYC regulations. In some countries, regulators have set the guidelines to the use of video conferencing as a way to securely onboard new customers.

Biometric devices for enrollment and authentication

To ensure convenience and a true cross-channel experience, mobile operators can propose assisted options for the enrollment and authentication processes. In these cases, customers are onboarded with the help of an agent, either in-branch or in the field, using biometric devices to capture biometric data (finger, face, iris). Dedicated devices can also be used to capture customer ID documents and electronic signatures.

Those powerful devices allow a multitude of applications such as enrollment (fingerprint, face, demographic data), document holder verification, local or remote processing, and digital ID creation to begin a customer journey with a telecom operator, and authentication to secure sensitive transactions.

MNOS as trusted identity providers

To comply with the strictest AML and CFT regulations and obligations, mobile operators offering financial services must also screen a customer's information against PEP (Politically Exposed Person) databases, or criminal, terrorist, and sanction watchlists. These verifications enable mobile operators to check if a user exists in any known watchlists maintained by governments, enforcement agencies, or public financial organizations.

Third-party database and verification services

Relying on extensive and accurate data sources not only provides an opportunity to positively verify customer identity, but also to augment the digital identity with new attributes. To achieve this, the digital identity can be cross-checked with a variety of trusted sources such as governments and public agencies, banks, credit bureaus, or utility service providers to ensure the information's validity.

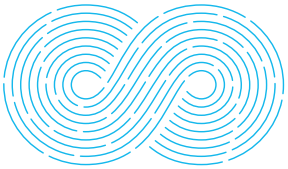
Identity management enables operators to develop a single, multi-channel profile for each subscriber that contains key identity attributes, customer preferences, and customer needs. With this information, mobile operators are in a better position to further engage with their customers and provide them with new offerings that are personalized to their needs.

Watch list management

Biometrics enhances watch list management by complementing alphanumeric identity verification with biometric matching against trusted databases throughout the identity lifecycle. Once the biometric attributes are created and stored (in compliance with local regulations), transactions may be verified against the stored biometric attributes, therefore providing an extra layer of security and assurance. Protection and privacy of biometrics must be ensured throughout their lifecycle.

Identity management

A comprehensive identity management solution gives mobile operators the ability to create, store, and authenticate digital identities with a high level of security. They are able to design identity workflow management to perform ongoing biometric data deduplication, identity attribute enrichment and aggregation, compliance and watchlist checks, manual adjudication services, and more throughout the identity lifecycle.



Key takeaways

In today's world, our digital identities have a lot of value. They enable mobile customers to access key services such as banking, eCommerce, health and travel, as well as perform administrative tasks such as enrolling for a new service, logging into an existing service, making changes to an account, or performing a remote payment.

Mobile Network Operators are in a unique position to provide digital identities to consumers: they have an unparalleled global reach, consumer trust, and huge amount of data gathered from mobile devices and their use by subscribers. Because of this position and responsibility, they are legally obligated in many countries to comply with KYC and AML regulations.

Despite these regulations, MNOs are still experiencing high rates of fraud – primarily driven by subscriber and identity fraud. With digital identity proofing solutions, they can turn their regulatory obligations into opportunities – 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.

A digital identity framework could be the differentiating factor that sets one mobile operator apart in today's highly competitive mobile market.

About IDEMIA

IDEMIA, the global leader in Augmented Identity, provides a trusted environment enabling citizens and consumers alike to perform their daily critical activities (such as pay, connect and travel), in the physical as well as digital space.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, an identity that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions, we reinvent the way we think, produce, use and protect one of our greatest assets – our identity – whether for individuals or for objects, whenever and wherever security matters. We provide Augmented Identity for international clients from Financial, Telecom, Identity, Public Security and IoT sectors.

With close to 15,000 employees around the world, IDEMIA serves clients in 180 countries.

For more information, visit **www.idemia.com**

Follow **@IdemiaGroup** on Twitter

We are **digital**

idemia.com/**we-are-digital**

IDEMIA

Join us on

www.idemia.com