Shufti Pro

Identity Verification

Automated ID Verification System to Tackle Telecom Frauds

White Paper

Outline

Evolution of Technology and Threats in Telecom Industry - An Overview

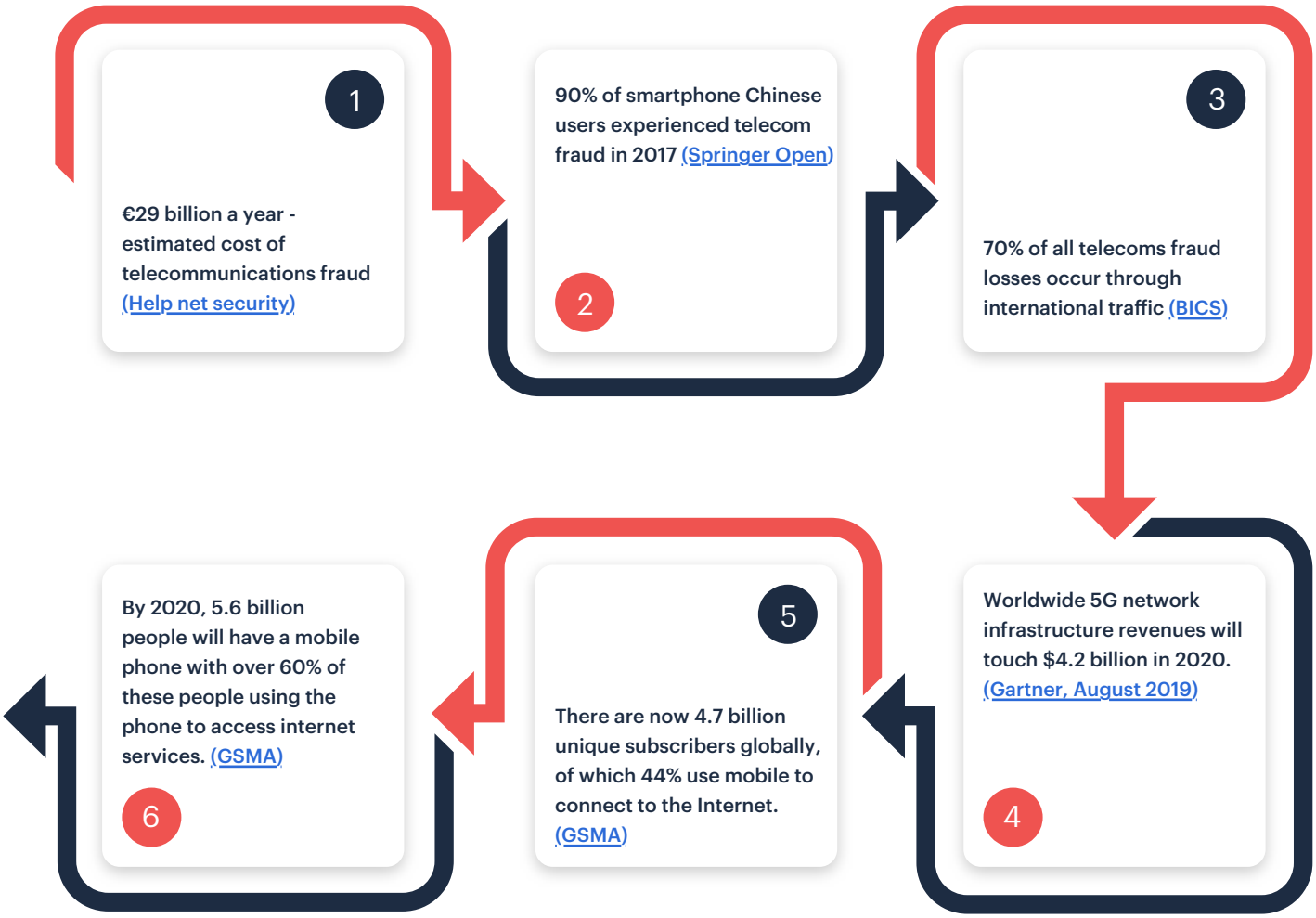
Telecommunications or telecom industry is a sector that continues to evolve and broaden in response to advancements in technology and the changing demands of consumers, as manifested in its increasing role and impact on the Internet Of Things (IoT) and the evolution of wireless technologies to 5G [1]. Telecom carrier networks are also poised to become Content Delivery Networks (CDNs), for instance, allowing users to load more internet content and transmit data at faster rates. Such developments need to continue since telecom influences how well we do business, provide services, broadcast information, and many other aspects of modern life.

As telecom services broaden in scope, so should our understanding of it, and a good place to start is its threat outlook, which is also expanding with the growth and evolution of telecom technology. Telecom-related threats and fraud cases exist largely because money is closely tied with telecom operations, where users have to pay for their telecom services. For all telecom services such as going online, making a call, or sending a message there is a fixed monetary value depending on the user's chosen carrier. This direct link to money is what really draws attackers or fraudsters who perhaps want to profit directly from the system or use it to launder their criminal revenue.

Presently, the telecommunications market is highly saturated with an extremely high switching rate. Telecom companies find it increasingly difficult to retain customers to come up with innovative services. Amidst all this, subscription fraud -- one of the most common telecommunication frauds -- is ever prevalent in this sector.

The annual cost of subscription fraud is estimated to reach over the US $12 billion, while many foresee the actual losses to be far greater, estimating it to be between 3% and 10% of the operators' gross revenues [2].

Therefore, identity verification presents itself as the perfect solution to counter fraud, in addition to providing a competitive edge to mobile service operators.



What is Subscription or Identity Fraud?

Identity fraud or subscription fraud happens when a fraudster uses fabricated identity documents to purchase or acquire telecom services to utilize them for future criminal activities. Criminals use stolen identities and credentials to purchase SIM cards, which later become a headache for Mobile Network Operators (MNOs).

As the services offered by MNOs flourish, the potential for subscription fraud increases too. Once a fake subscription is established, the criminals then have access to a wide range of value-added services including not just call-related, TV, and internet, but also new mobile financial services such as mobile banking and mobile payment. CFOs and heads of fraud departments for the major network operators are facing huge challenges to secure the channels under fraud threats. **According to risk management and analytics experts of Neural Technologies, there are over 200 types of telecommunication fraud, related to identity theft or fabrication [3].**

How does it happen?

During the consumer acquisition stage in the MNO's store in Europe or Asia Pacific countries, consumers have to provide identity documents (such as id-card or driving license), or passport, and if you are a tourist you may need to present proof of address as well [3]. Identity verification service is an essential part of the subscription process and is usually carried out manually by a sales assistant. However, the manual checks performed by official members can
be ineffective and lead to errors.

In case, if the company official fails to detect forged or stolen documents during the customer onboarding, the fraudsters can manage to walk out with high-end and heavily subsidized smartphones that may take some time before the fraud is discovered.

Similarly, SIM-swap fraud is another major issue, whereby scammers use fake IDs to gain access to a legitimate subscriber's SIM card. Those stolen SIM cards are then used to authenticate transactions with the real subscriber's bank, making online purchases, money transfers, and running up huge costs in the legitimate subscriber's name. These kinds of errors usually occur while performing manual identity verification, which can prove to be ineffective and exposes customers to a major risk of telecommunication fraud

This in-return creates a sense of distrust amongst customers when they find their credentials are being used fraudulently to commit subscription fraud.

Shufti Pro not only reduces the risk of identity fraud in the telecommunication sector but also establishes a seamless customer experience with AI-based automated identity verification solutions capable of verifying an end-users in 15-60 seconds.

Why Strong ID Verification is Critical For Network Operators?

Effective identity verification solutions are the key to tackle telecom fraud. The Technology Research Institute states that ***"real-time point-of-sale identity verification services are an invaluable aid to stopping fraudsters from exploiting identity theft."***

MNOs face a massive challenge in this regard; they have to overcome fraud while staying compliant with local and international regulations. Their CFOs and revenue assurance departments need to reduce the heavy financial burden of fraud and protect their brand image to maintain their reputation as operators one can trust.

Compliance and regulations

Governments and public security authorities are requesting network operators to perform stronger identity verification to combat fraud and criminal activities. For example, more than 90 countries now have to perform proper registration with strict identity verification for the purchase of prepaid SIM cards to tackle national security issues and criminal behavior, following recommendations from the GSM Association (Global System for Mobile Communications). **Compliance is critical for MNOs, especially as prepaid SIM cards represent 47% of the global SIM card market [4].**

GSMA Regulations in the United States (US) that are applicable to MNOs include:

- Regulation of entry and service provision
- Regulation of interconnection
- Regulation of price cap

GSMA recommendations

GSMA in its paper published in 2016 suggested the following recommendations for policymakers when considering the introduction, or revision, of a mandatory SIM registration policy [4]:

- Consult, collaborate, and communicate with MNOs before, during, and after the implementation exercise, while balancing national security demands against the protection of citizens' rights
- Place realistic timescales for designing, testing, and implementing registration processes
- Provide clarity on registration requirements before any implementation
- Allow and encourage the storage of electronic records and design easy registration processes
- Allow and encourage the registered ID to be utilized for other value-added mobile and digital services
- Support mobile operators in the implementation of SIM registration procedures by contributing to joint communication activities and to their operational costs

Furthermore, mobile financial services are playing a progressively important role in the service offer from MNO's portfolios, and therefore they must meet Know Your Customer (KYC) ID verification procedures as well. Non-compliance with such regulations can lead to fines and disablement of SIM cards and services.

Know your customer:

As of December 2018, around 150 governments imposed KYC regulations on MNOs that require customers to provide a valid proof of identity through a government-issued or recognized credential [5], such as a national ID document or passport to subscribe to any mobile services. Governments take different approaches to implement SIM registration policies, but these regulations generally fall into one of the following three categories:

Storing data

Mobile network operators are required to capture and keep a record of a set of personal information about the SIM user (hat information can vary from jurisdiction to jurisdiction). About 85% of the countries performing SIM registration follow this approach [6].

Sharing with authorities

MNOs are required to proactively capture and share the SIM user's personal information with the government or regulator and around 4% of the countries mandating SIM registration follow this approach [6].

Validating

Network operators have to validate their customers' identification information against a central government database which is usually maintained by a government authority or regulator. Only 16 countries (11%) mandating SIM registration follow this approach, out of which 11 countries (7%) also require service providers to use biometric authentication verification when registering their prepaid SIM customers [6].

The financial burden

Telecommunication fraud resulting from insufficient identity verification procedures can take months to be discovered. Such frauds result in considerable financial losses for cellular operators that are both direct, with the loss of a heavily subsidized handset, and indirect, through all the services an MNO offers with a single subscription including foreign calls, internet, TV, and mobile financial services.

According to Neural Technologies, the estimated annual cost of identity fraud in the telecoms industry is €40 billion [3].

Damaged brand image

In addition to the financial losses a company has to incur, increased fraud cases can severely damage the reputation of a telecom company with customers losing their trust in them. MNOs must act fast to address the damage caused to their reputation as a result of poor user experiences.

This can include compensation and incentive payments, updating of security layers in back-end systems, and issuance of SIM cards by following proper verification procedures.

Traditional practices for customer ID verification

Most telecom companies are currently using standard, in-person verification for customer authentications, and several of them have nearly non-existent identity verification measures. Ineffective measures for users' verification before issuing them service has highly detrimental costs for MNOs.

Moreover, the legal exposure that comes with allowing criminals to use telecom services to commit fraud is huge. The growing use of unverified SIM cards for illicit activities that range from kidnapping to terrorism also has regulatory authorities on edge. Therefore, all network operators are encouraged to fulfill Know Your Customer (KYC) regulations effectively.

Benefits of Automated ID Verification

Reduced friction in customer onboarding

Online ID verification is faster and more reliable which is immensely helpful in reducing friction and drop-off rates during the customer onboarding process. Many customers find manual onboarding procedures slow and according to a report, 76% of mobile network subscribers prefer single sign-on service from their mobile operators [7].

Moreover, the added possibility of errors caused by manual processes can increase their frustration, thus causing them to abandon the process entirely. Here automated verification solutions can be very helpful as they allow for instant onboarding procedures by electronically extracting data from IDs, thus enabling frictionless customer onboarding procedures. This further helps in improving customer service operations, thereby establishing customer-centric organizations.

Enhance efficiency

An automated identity verification software uses OCR technology to extract data from scanned documents, increasing efficiency, and thus completely eliminating the need for manual verification procedures. The customer's identity is further verified through biometric facial recognition. It eliminates the need for in-person verification and consumers can register for services from the comfort of their home. All these features combine to streamline operations for the telecom sector, thus increasing their levels of productivity and security.

Better security

By implementing automated or digitized identity verification solutions, MNOs can increase the level of security during the customer onboarding process. Such systems can identify a fake ID within seconds, enabling telecom companies to detect fraud instantly. Automated verification systems are equipped with identifying standard government-issued ID documents from several countries, therefore, making it near impossible for the perpetrator to commit subscription fraud. Facial recognition eliminates the risk of some highly advanced identity frauds such as synthetic identity by comparing the live photo of a consumer with his photo on verified identity documents. The digitized verification process is highly effective as it counters spoof attacks and can identify photoshopped images as well.

Building customer loyalty

By implementing proper and active security measures, MNOs can secure customer data, their identities and can establish trust amongst users thus increasing customer loyalty. Along with increasing security in their systems, telecom operators can also comply with government regulations, requiring companies to verify customers properly and to keep records of those verifications. This can help companies to enhance their reputation in the market and build trust amongst regulators as well.

How Shufti Pro is Helpful?

AI-based identity verification solution

Shufti Pro is a KYC verification service provider that offers identity verification services through an AI-powered verification engine. It utilizes a hybrid technology of AI and Human Intelligence to verify users within seconds. It also has universal language support that allows it to cater to users and clients from all over the globe.

Shufti Pro offers the ultimate telecom fraud prevention guide to MNOs and helps businesses in the seamless onboarding of their customers. ID verification from Shufti Pro is the ultimate solution for businesses looking to reduce fraud and enhance their operational efficiency.

Identity verification process

Shufti Pro is an API based identity verification solution that approves real customers in seconds to increase conversions, reduce chargebacks, and deter fraudulent attempts. Through its real-time document verification and online facial recognition, Shufti Pro is able to verify global users accurately and seamlessly.

Document verification

Shufti Pro's document verification enables quick and secure enrollment of customers with a 98.67% accuracy rate. It supports 3000+ types of ID documents in 150+ languages and can verify government ID cards, passports, licenses, and credit/debit cards.

Shufti Pro verifies customers' documents in 4 simple steps:

- User takes a photo of his identity document in real-time or uploads a photo from mobile
- Shufti Pro's solution extracts required information using precise OCR technology
- Performs authenticity analysis of the ID document using AI and HI
- Sends verification details to the client via API or back-office

Shufti Pro's state of the art Optical Character Recognition technology extracts accurate information from various documents with complex characters and performs various checks to confirm a document's authenticity.

Facial recognition

Shufti Pro's facial recognition technology utilizes AI and HI to perform customer verification in just 5 seconds. The software captures the picture of the customer in real-time and matches the facial checks with the ones stored in the database. The following images elaborate on how facial recognition is performed.

Facial recognition process

Shufti's facial recognition technology can help telecom companies to identify various frauds with the following checks:

- Liveness detection
- Microexpressions analysis
- 3D depth perception
- Anti spoofing checks
- Fake image detection
- Human face attributes analysis
- AI mapping techniques

Ongoing KYC

Through Shufti Pro's biometric authentication network operators can enroll users with swift biometric sign-in using face and ID recognition and can use that information to approve their users' future transactions. Shufti Pro's Ongoing KYC allows end-users to sign-in into their accounts with just facial recognition, this saves them from the manual password-based procedures and delays.

With all the regulations in place, it is mandatory for every network operator to perform ID verification procedures to ensure their customers' authenticity and secure the existing data of their users. In this regard, Shufti Pro presents an all-in-one ID verification platform for telecom operators to streamline their onboarding processes and ensure security. Shufti Pro can be easily integrated into your businesses in order to verify all existing and recurring customers.

Simple API integration and your business will be empowered to verify remote customers from all over the world without sacrificing customer security or data privacy protocols.

Learn how Shufti Pro can streamline your customer onboarding process

Discuss it with our experts

Or apply for a no-commitment free trial

Get non-discriminatory access to all features of the selective service of Shufti Pro for 15 days.

Get a Free Trial

www.shuftipro.com

sales@shuftipro.com

Resources

1 https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/global-telecom-crime-undermining-internet-security-cyber-telecom-crime-report

2 https://www.linkedin.com/pulse/subscription-fraud-mother-all-telecom-frauds-shankar-palaniandy

3 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/05/Understanding-Capture-and-Validate-KYC-Processes-Web.pdf

4 https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/identity-fraud-in-telecomunication

5 https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

6 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/05/Understanding-Capture-and-Validate-KYC-Processes-Web.pdf

7 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf

8 https://owmobility.com/press-releases/76-subscribers-interested-single-sign-services-mobile-operator/

9 https://www.helpnetsecurity.com/2019/03/22/telecommunications-fraud/

10 https://events.capacitymedia.com/event/b689568c-b59e-4f23-926b-439e4b2d3439/summary

11 https://bics.com/no-mobile-operator-is-an-island-in-the-threat-of-telecoms-fraud/

Shufti Pro

True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.