thalesgroup.com

THALES
Building a future we can all trust

# Thales Trusted Digital ID

## Where robust ID fraud prevention meets a seamless customer journey

# TABLE OF CONTENTS

# Thales Trusted Digital ID
# Where robust ID fraud prevention meets a seamless customer journey

## Executive Summary

Identity fraud is increasingly recognized as a business-critical issue for Mobile Network Operators (MNOs). However, the structures and strategies typically employed by MNOs often hinder attempts to identify the scale of the problem and address fundamental security weaknesses. Moreover, standard mitigation techniques are of limited value in terms of deterring well-organized and sophisticated fraudsters.

Traditionally, MNOs have essentially treated the problem as one of risk management. All too often, the result is a security solution that not only fails to prevent fraud, but also undermines the customer experience. In this white paper, we explore the nature of the threat posed by fraud, and the true costs being imposed on MNOs. We also introduce a new approach to fraud prevention that can embrace genuine consumers while resisting criminal attacks. Combining real-time ID document verification with seamless biometric authentication, Thales Trusted Digital Identity enables MNOs to slash fraud losses, enhance the customer experience, and automate routine administrative processes.

## Business context

Mobile Network Operators (MNOs) face unprecedented levels of competition and commercial pressure. In response, many have created extensive service portfolios, extending far beyond mobile communications. At the same time, the number of channels deployed to reach subscribers is also multiplying, encompassing the internet, mobile apps and voice calls. As a result, MNOs must address the challenge of managing ever-greater complexity.

Almost inevitably, the wealth of valuable services now offered by operators has attracted the attention of sophisticated fraudsters. Furthermore, a multi-channel environment provides these criminals with greater opportunity to target potential weak points and launch successful attacks on a business and its customers.

The figures speak for themselves. According to the Communications Fraud Control Association (CFCA), f**raud is costing the global telecoms industry in excess of $30 billion every year**. Many operators are losing **as much as 5% of their revenues** to this increasingly well-organized criminal activity. Within this, **subscription fraud** (a form of identity fraud) is a particular problem, **accounting for 35-40% of all such losses.**

Under any circumstances, this drain on financial resources would demand a reaction. But in an economic environment characterized by uncertainty and disruption, tackling fraud has quite simply become a priority for every MNO.

## Know your enemy: understanding different types of identity fraud

Any successful fraud prevention strategy is built around an understanding of the multi-faceted threat posed by modern criminals. As the range of services offered by operators expands, so do the rewards of successful ID frauds. The fraudster aims to access to a wide array of value-added services including subsidized handsets, TV and internet, gaming and music. Even more dangerous is the potential to reach security-critical services such as mobile banking and mobile payments. Increasingly, these are an integral part of the MNO offer.

Generally speaking, identity-related frauds enable either the fraudulent use of telecom services, or the use of such services for subsequent fraudulent activities. They fall into three main categories:

1. **Subscription fraud**

### How does it work?

Whether it is performed face-to-face in the MNO's store, or remotely online, during the consumer acquisition stage the prospective subscriber must usually present an ID document, as well as utility bills and their bank account details. But without an effective method of verification, the potential for subscription fraud is clear. The fraudster's immediate aim is to use the MNO's services without paying. This can be achieved by either using completely falsified ID documents, or a genuine ID document with the photo swapped. Often this type of fraud occurs when a sales representative, understandably keen to preserve the customer experience, accepts a document without credible assurance of its authenticity.

Both postpaid and prepaid offers are vulnerable. For postpaid, the applicant's aim is to obtain a subscription and related services and/or a mobile device, with no intention of paying. For prepaid, in countries where registration is mandatory, the objective of fraudsters is a phone line that allows them to remain anonymous.

## 2. Account takeover

Account takeover is another significant type of identity fraud. As the name suggests, fraudsters use the genuine accounts of their victims to access the MNO's services.

### How does it work?

Fraud can occur using information gathered through social engineering of a genuine customer.

Customers are tricked (e.g. via phishing attacks) into providing information regarding their account. This information may then be used to contact an MNO's customer service department and impersonate the customer. It can also be used for compromising online accounts, and in retail stores.

Common to all account fraud is the desire to exploit weaknesses in an MNO's customer service operation. Often this will take place over the phone, particularly if call centres are delivering services based on ineffective methods of identity verification. However, account takeover can also occur via online channels, or physical channels where the fraudster uses false or stolen ID documentation.

One of the most common types of account takeover fraud is the so-called SIM-swap. For MNOs and their customers, this has become a major concern.

### How does it work?

Scammers impersonate a customer to gain access to a legitimate subscriber's SIM card. They then use this SIM 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.

## 3. Dealer fraud

This covers any activity by a dealer, contracted to provide sales or distribution services to an MNO, that is in fact intended to deprive that operator of revenue. A dealer typically commits or knowingly assists fraud against the MNO or service provider in order to increase commission payments. In many cases, the fraudster is not actually the owner of the store, but an employee seeking to boost their income.

In such cases, a dishonest sales channel, or sales channel employee, may use genuine customer information (e.g. activation lists) to open new lines or accounts without customer authorization.

Alternatively, a dealer may collude with criminals in establishing fraudulent subscriptions, by knowingly validating false customer identity and credit checks at point of sale.

For fraudsters, the proceeds can include increased commission and the opportunity to resell subsidized handsets.

**"(It is) difficult to assess precisely the cost of fraud but this could represent up to 5% of the company's revenues; within that 5%, 30% of fraud can come from employees, for sales commissions."**
Head of Security Operations, major global MNO

## Navigating the identity fraud maze

For MNOs, there are two key reasons why the fight against identity fraud is becoming more complex. The first is the proliferation of channels through which customers now interact with them. The second relates to internal organization, in the form of the numerous 'silos' within the MNO's structure that are involved in fraud prevention.

### More sophisticated, multi-channel threats

Securing all the channels that fraudsters can target represents a major challenge for CFOs and fraud departments. According Neural Technologies, a risk management and analytics expert, there are over 200 types of telecommunication fraud, all related to identity theft or fabrication.

In many respects, new regulations that demand stronger ID verification have simply raised the bar for in-store fraud. In response, criminals are employing more sophisticated techniques, such as the use of high quality, fake ID documents. Moreover, the fight against fraud is taking place at a time of profound digital transformation. Physical stores may remain a significant touchpoint for many consumers, but as in other industries, a major shift to the online domain is now well advanced.

A recent paper from Capgemini*, produced in partnership with Vlocity (a Salesforce company), vividly illustrates the strategies being pursued by a new breed of Digital Mobile Network Operator. Right around the world, these innovative business models are reshaping the B2C value proposition through the creation of 100% digital experiences for their customers. (* Digital Operator Observatory B2C Focus, 2020).

Another Capgemini survey reveals the key role that remote ID verification plays in making these new digital-only brands a reality. In particular, *"The Connected Telco Consumer: How Telecom Operators Can Reconnect With Customers and Emerge Stronger From the Pandemic"* highlights the use of biometrics such as facial recognition to enable quick and easy processes for registration and connectivity activation.

### Consumers share the pain

The impact of fraud is felt by consumers as well as businesses. In 2019, Thales conducted a survey of 810 consumers across eight countries worldwide. "*Making Trusted Digital IDs a Reality: What Consumers Really Think*" revealed that almost half had already had their ID compromised. The security and privacy issues experienced include having personal data such as their name and date of birth stolen, credit card details accessed and social media accounts hacked. Overall, 67% feared having ID-related details stolen.

### Missing the bigger picture: how internal silos can undermine fraud prevention

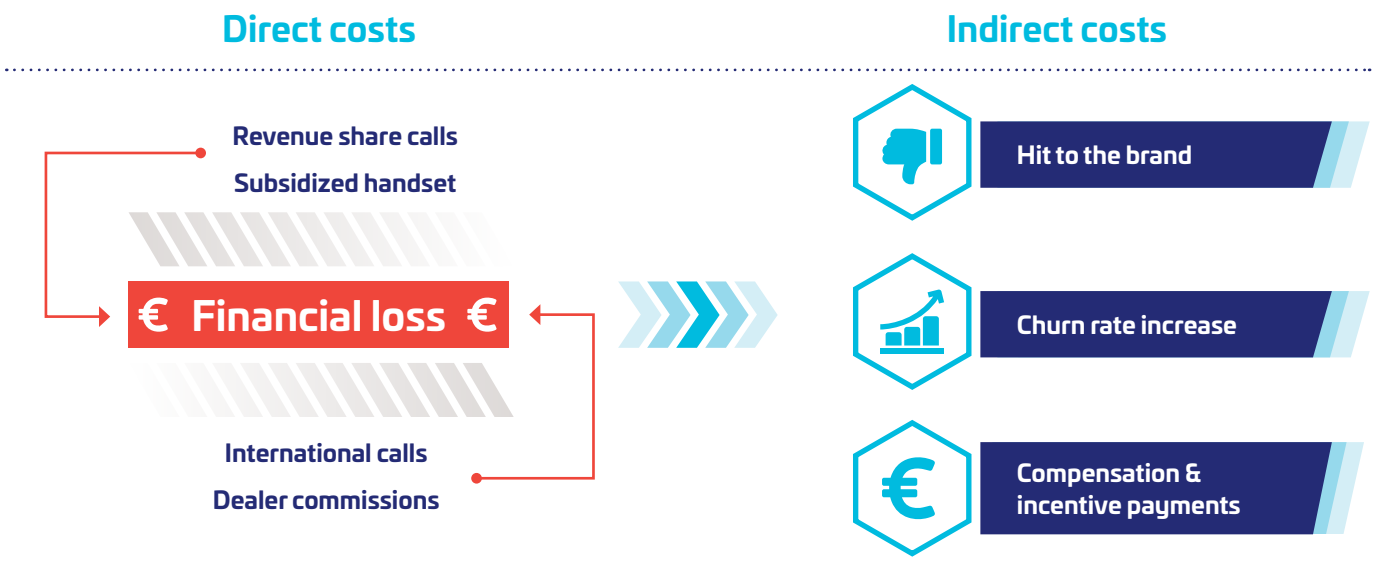
Multiple 'silos' within an organization can seriously undermine attempts to stem the flow of losses to fraud. The heart of the problem lies in the fact that responsibility for measuring the impact of fraud, and implementing solutions, is split across several departments: fraud; revenue assurance (RA); credit risk; IT security; network security. Each will have their own KPIs and objectives. And it is quite possible that none will have a 360°view of the scale of fraud across the organization.

Clearly, good communication and coordination is needed between all stakeholders. Indeed, a number of major global MNOs have now created structures within which different departments, including product marketing, are brought together to address RA and optimize fraud prevention.

> **"The average duration before frauds were discovered could be three months."**
>
> Head of Security Operations, major global MNO

## The iceberg effect: measuring the direct and indirect impacts of identity fraud

When assessing fraud, it is vital to look beyond the direct costs incurred. Indirect costs can also have a dramatic impact on the bottom line. Indeed subscriber dissatisfaction, not only hit the brand but can lead to churn rate increase. Additionally, indirect impacts include compensation and incentive payments, updating of security parameters in backend systems, and reissuance of SIM cards. Any financial liability issues with banks must also be taken into account. In high profile cases, restoring trust with consumers, investors and partners may necessitate long and costly advertising campaigns.



**Staying focused: what fighting ID fraud should really mean for MNOs**

For MNOs, there is an obvious temptation to see the fight against fraud as a case of catching the 'bad guys'. In reality, the focus needs to be on metrics such as revenue, customer satisfaction and subscriber growth. MNOs should also develop an understanding of the criminals' business models, and aim to make the cost of a successful fraud attack too high to be worthwhile.

To achieve this, MNOs need to have the following objectives in place: prediction, detection, action. In practice, that means:

- Increasing visibility of fraud losses across the business
- Ensuring early detection of new fraud risks
- Establishing proactive strategies rather than reactive measures

Ultimately, the equation for operators is as simple as this: **cost of fraud vs cost of protection.**

## Traditional fraud mitigation methods combine weak security with a poor customer experience

When enrolling customers, MNOs currently employ a variety of different mitigation methods to minimize the risk of subscription fraud. These include manual ID verification, which is frankly of limited value in terms of detecting fake documents. Another approach is to adopt precautionary measures whenever there is doubt over the credibility of ID credentials. However, this inevitably comes at the expense of the customer experience. Typically, services are restricted for a period of time after the subscription is activated. For example, the customer is denied access to roaming services and international calls. Effectively this buys the MNO time to perform ID verification and credit checks. In extremis, the MNO may simply decide to reject a subscription application rather than run the risk of fraud.

As far as account takeover fraud is concerned, MNOs can employ further strategies to confirm the identity of a person calling the customer service department. For example, security questions can be asked to check that the answers match those recorded by the genuine customer when their account was opened. These help to back up the usual questions such as name, date of birth and address. Several other mitigation methods are also available, but all these techniques have inherent drawbacks for both MNOs and end users. On one hand they are not particularly effective, and increase the risk of losses caused by fraud. At the same time, they inflict significant damage on the customer experience.

**For MNOs**

- Financial losses due to ineffective fraud mitigation
- Sales reps spend time on non-valuable tasks
- Loss of revenue due to downgraded services
- Risk of churn due to poor customer care experience

**For customers**

- A compromised experience, with delays at every stage of the journey from subscription request right through to after-sales customer care

## Fighting fraud with Thales Trusted Digital Identity

Thales Trusted Digital Identity platform spells an end to the trade-off between security and the customer experience. Unlike mitigation methods, we offer an effective, systematic and secure approach to fighting fraud and streamlining the customer journey. Crucially, this encompasses onboarding smoothly across all channels, in-store and online, right through to service access.

We resolve the dilemmas faced by MNOs by using automated, reliable processes that are built on state-of-the-art ID document verification. What's more, we employ advanced biometrics checks to verify identities and authenticate and identify customers.

All these verification solutions are part of **Thales Trusted Digital Identity platform.**

Below we illustrate the two main types of verification: ID document and biometrics, which can be further completed by risk management for additional layers of security. Typical use cases are also highlighted. Note that right across the world, Thales' implementations comply with local regulations related to data protection and privacy.

**1. ID Document verification**

Thales real-time ID Document verification solution is used to determine if a prospective customer is presenting valid identity credentials. As a result, it strengthens an MNO's defence against the threat of subscription fraud, and the revenue losses that occur when a high value handset is handed over to a criminal. Furthermore, Thales' approach to ID verification is highly flexible, improves the sales process, and can help speed and automate routine administrative tasks. ID verification can be applied at the point of subscription for a new customer, or when an existing subscriber wants to upgrade or change their plan. Moreover, verification can take place either online or in-store.

Dedicated software is employed to verify the authenticity of ID documents, with a variety of methods available to check security features against Thales' comprehensive ID database. Operators can also choose from different levels of verification:

**Standard verification** is based on the ID picture in visible light, and can be used both in-store and online; document capture is performed either by a simple scanner, or via a smartphone or tablet.

**Advanced verification** is primarily designed for use in-store. Advanced readers enable verification of security features that can only be seen in white, infra-red or ultraviolet light, as well as chip-based verification of electronic documents.

In both cases, the document holder's personal information can be extracted automatically to populate the fields in registration forms and the CRM, for example. MNOs and their customers therefore benefit from a faster and simpler onboarding process. The operator also reaps significant time savings and, by eliminating the risk of human error, more accurate data entry.

### 2. Biometrics verification

#### Does the face fit?

For online subscriptions, ID document verification only represents part of the solution. To verify that the person presenting the document is who they claim to be, the use of biometrics such as facial matching becomes a necessity.

Thales' facial matching solution performs a comparison between the photo printed on an identity document and a live capture of a face (front-facing or selfie). A smartphone, web camera or tablet can fulfill the role of the face capture device.

Thales' software manages the capturing process. It also implements comprehensive liveness detection to prevent fraudsters from using a myriad of techniques to try to fool the system. These include printed photos, images broadcast from a screen, animated videos, 3D 'hard' masks, head sculptures and other mechanisms employed to fake identities.

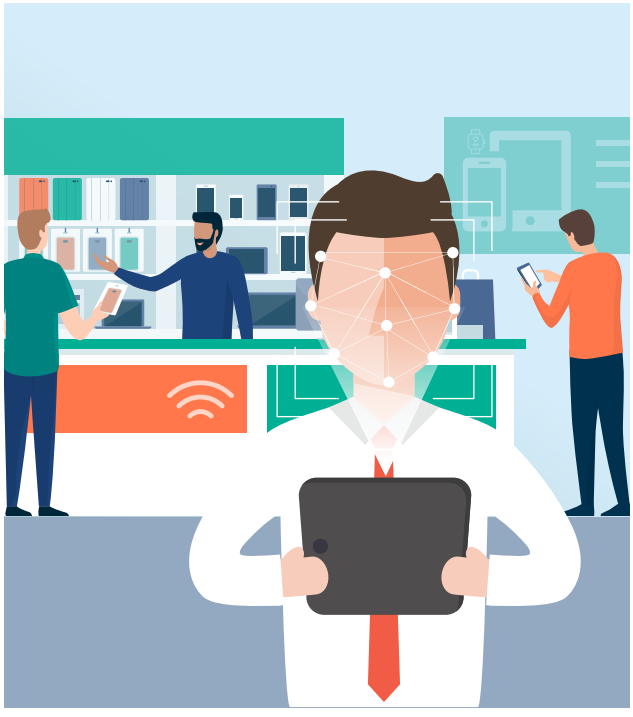
Liveness detection can either be employed in 'passive' mode, where it is completely transparent for the end user. Alternatively, the MNO can choose a solution that requires the subject to move on request, for example blinking their eyes or tilting their head.

Results are provided in seconds; the face image captured is sent to the verification service for analysis in the backend. This determines whether there is a match between the selfie and the image on the ID document.

#### Time to forget about passwords

To address account takeover fraud and enhance the customer experience, Thales' solution can replace traditional login/password methodologies with effortless, biometric-based authentication. When customers want to access their services, face or voice matching with liveness detection is employed for remote biometric authentication. The relevant biometric attribute is compared instantly with the information stored on the MNO's database.

#### Dealing with dealer fraud



Thales' solution provides a biometric-enabled method of authenticating employees and resellers when accessing an MNO's services. This prevents dealer fraud, and fraudulent use of the means of identification for employees and resellers. Again this can be achieved through seamless facial or voice matching, supported by liveness detection.

### Shutting the door on fraudsters

Biometrics can deliver robust protection against face-to-face attempts at account takeover fraud. Identification takes place automatically in-store, and an individual's biometrics are compared with known fraudsters held on a database. Apart from fraud, this approach can also be employed to recognize returning customers, enabling personalized service, VIP treatment or eliminating the need to queue.

### The right call for customer verification

Biometric voice matching is a highly effective means of identifying attempts by fraudsters to impersonate genuine customers when contacting call centers. Drawing on the numerous different features that together define the uniqueness of an individual voice, this approach quickly compares a speaker's recorded voice with thousands of similar recordings held in databases. By matching a caller's voice with information such as the recordings of known fraudsters, it is possible to address the threat of account takeover before it becomes a financial liability for the MNO.

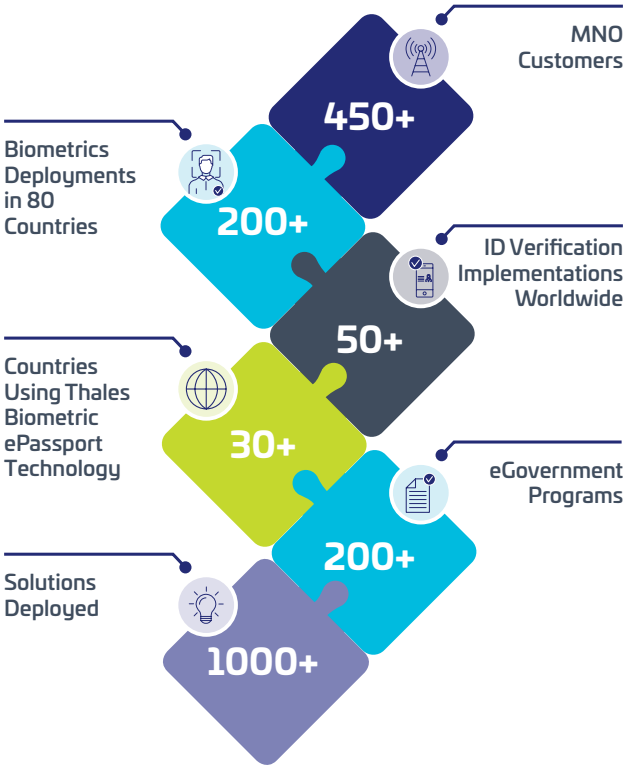
Thales' solution is capable of analyzing all calls recorded by the MNO and comparing them to archive recordings. Furthermore, it is unique in working with both mono and stereo recording data.

### 3. A flexible approach to risk management

For both first-time enrolment and authentication, an additional layer of security can be adopted. Highly flexible risk management systems are a key element of this approach, reflecting the constantly evolving and increasingly unpredictable nature of cyber threats. Responding to new situations and implementing adaptive security policies, these systems can detect issues such as unusual locations and user transaction patterns, evaluate the risks, and remotely stop the transaction or request further verification. Crucially, this analysis is executed in real-time. Threats are counteracted immediately, before they become financial liabilities.

The additional security layer relies on a mobile app collecting and sending context-based data to a risk management server for analysis and processing. This data includes device-related information (e.g. serial number, IMEI, OS version), root / jailbreak detection, and user behaviour such as transaction patterns and geo location. After analysis by the risk management server, a reputation score linked to the device and user behaviour is established and an immediate decision is made to either accept or reject the transaction, or request further verifications, based on the security policies applied by the client.

## Why Thales?




Thales makes the digital customer journey an experience we can all trust, whatever your industry, wherever you operate, through a range of products and services that:

- **Connect** and manage devices
- **Protect** devices, identity and data
- **Predict** to build a resilient network

THALES

Building a future we can all trust

> Thalesgroup.com/Mobile <