infobip

Flash Calls

A new source of revenue for MNOs?

With Anam Inside

INTRODUCTION

This white paper deep dives into the recent emergence of Flash Calls as a method used by global smartphone apps to verify mobile numbers. A2P SMS is the de-facto method due to reliability and quality of delivery, so much so that International A2P SMS traffic volumes are dominated by One Time Passwords (OTPs) and PINs.

Based on a comparative study of the different verification methods including Flash Calls, the paper concludes that the key differentiator for a brand to choose Flash Calls as the “in-app” number verification method is cost, which is evidenced by its emergence in markets where the International A2P SMS price is high.

Finally, the paper explores different strategies for MNOs to consider when monetizing their network assets for phone number verification. Securing deserved revenue streams requires a combination of pricing strategy and securitization techniques to ensure a sustainable service for both MNOs and businesses alike.

Contents

CURRENT STATE OF PHONE NUMBER VERIFICATION

The digital economy is continuously advancing and becoming a normal part of our lives. More and more enterprises, OTTs and social media companies are communicating and interacting online with their customers predominantly via mobile devices. Mobile communications have evolved with hi-speed smartphones in addition to the traditional voice and SMS channels that have existed since the 90s and the 2G era.

The widespread use of mobile communications has meant that fraudsters have now turned their attention to attacking any weakness in this channel. To counteract this, enterprises have increased the authentication and verification steps to secure mobile engagement with their customers.

An important part of any business consumer relationship is the “account” and the different forms of sign-on and authentication mechanisms that goes with it. As mobile communications are an inherent part of digital engagement, the mobile number (also known as the MSISDN) is seen as a trusted identity due to its inherent association with a securely issued SIM card. Therefore, it is often made an element of the account profile data. Many use cases exist where verifying a mobile number (MSISDN) is needed, including:

- Account creation, where the business is verifying that a new customer is in possession of a MSISDN
- Sign-in, where the authentication process proves the possession of the MSISDN linked to the already created account
- Password change or reset due to forgotten password and the business is using 2FA to verify the user.
- Switching devices. In this case, apps will need the user to sign-in again with existing number or new number depending on the context of the device switch by the customer.

While some solutions exist for a mobile network to provide an authenticated MSISDN as part of the customers communication over the cellular data channel, these are not universally available (e.g. when the customer is interacting with a brand via their desktop).

The most common method in use today proves that the customer is in possession of the MSISDN by delivering a “one time PIN” (OTP) to the same MSISDN; the method is further secured using the MNO network leveraging the fact that the MSISDN is an authenticated entity inside their domain.

The most common methods are summarized below

Method	How it works	User Experience
A2P SMS 	An A2P SMS containing the OTP/PIN is delivered using the business messaging ecosystem to the MSISDN. The OTP/PIN is then supplied to the mobile app (or web page) to verify the MSISDN.	Some android apps can auto copy the OTP from the SMS received and verify the MSISDN. iOS apps may provide a one-click prompt to auto-copy the OTP. Otherwise, the customer needs to enter the OTP/PIN manually to complete the verification. If in the case that the SMS is delivered over official channels, the message text will contain the brand name. In some countries, the brand name is also present as the Sender ID when alpha Sender ID is allowed.
Text-to-Speech Call 	An IVR-like system sets up a voice call to the MSISDN that needs to be answered by the customer. Once answered the OTP/PIN is read out using a TTS component.	The customer must answer the call, listen, and note down the read-out OTP. Any branding would be within the TTS content that is read out to the user.
Flash Call 	A Flash Call provider sets up a voice call towards the MSISDN. The OTP is contained (somewhere) in the calling line identification (CLI) digits. The app that is verifying the MSISDN drops the inbound call and reads the phone's missed call log to retrieve the OTP from the CLI digits.	This method can only be used by mobile apps that have been allowed access to the phone's missed call log. The customer does not need to answer the call or read the OTP. This seamless user experience is currently supported only on Android devices.

In all these cases, the verification method is using the trusted network of the MNO to reach the MSISDN and convey an OTP to it.

INTERNATIONAL A2P SMS AND OTP

Differentiation of the A2P SMS product into “International A2P” and “Domestic A2P” has become common in most global markets.

“International A2P”

usually means SMS messages initiated by organizations who have a global customer (or active user) footprint. This includes OTT providers (e.g., WhatsApp), Social Networking brands (e.g., Facebook), global FinTech apps (e.g., Binance).

“Domestic A2P”

usually means SMS originated by local businesses such as national banks, online microfinance institutions, local retailers, etc.

Initially this differentiation was introduced to allow MNOs in these regions to gain extra wholesale SMS revenues for A2P SMS.

Although there is no uniform definition of what qualifies an A2P SMS as “international originated”, most MNOs categorize it based on the brand (rather than the aggregator/CPaaS provider) that is sending the SMS to the customer.

“Value” of the SMS content can also play a part, for example promotional traffic from international brands is charged per domestic rate as the promotional message is not considered business critical or time critical to commercially justify paying a higher rate.

We performed a study of the most common A2P SMS use cases sent over international channels across three MNOs spread across the regions. We learnt that A2P SMS conveying OTPs represents over 90% of all international A2P SMS.

MNO Region	Verification/2FA	Notifications	Other
Africa	89.68%	5.81%	4.51%
Asia	92.52%	4.29%	3.19%
Middle East	75.75%	7.08%	17.16%

Further analysis reveals that most brands sending 2FA SMS are OTTs, social media companies, fintech apps and ride-sharing apps (eg Grab, Uber, Bolt, etc) whose customers are spread over many countries. These online companies are engaging with their customers mainly by using mobile communications, with a large volume of OTP SMS reflecting the different authentication and verification use cases mentioned earlier.

INTERNATIONAL A2P SMS PRICING TRENDS

Most MNOs that introduce such traffic segmentation to improve their A2P revenue have sought to secure the expected revenues against "grey route" loss by deploying SMS Firewalls in their networks. This has resulted in secured and maximized revenue streams. However, in recent years there has been a trend by some MNOs to grow this revenue stream by steadily increasing the price of international A2P SMS knowing that the grey route threat is under control[1]. This price increase has also helped to recover some of the losses associated with roaming revenues which were severely impacted during the Covid-19 pandemic.

This price trend has resulted in huge cost pressures on businesses who use (and ultimately pay for) international A2P SMS. Given that OTPs constitute over 90% of the use cases for international A2P SMS, these businesses are seeking (in conjunction with their messaging providers) to explore other channels. This search for cost-effective, alternative methods is not unexpected – in fact it is the classic example of the "substitution effect" in economics.

The product that emerged due to this substitution effect in 2022 is Flash Call verification. Even though this method has been around for a few years, businesses are beginning to consider using this method in high-price A2P SMS markets.

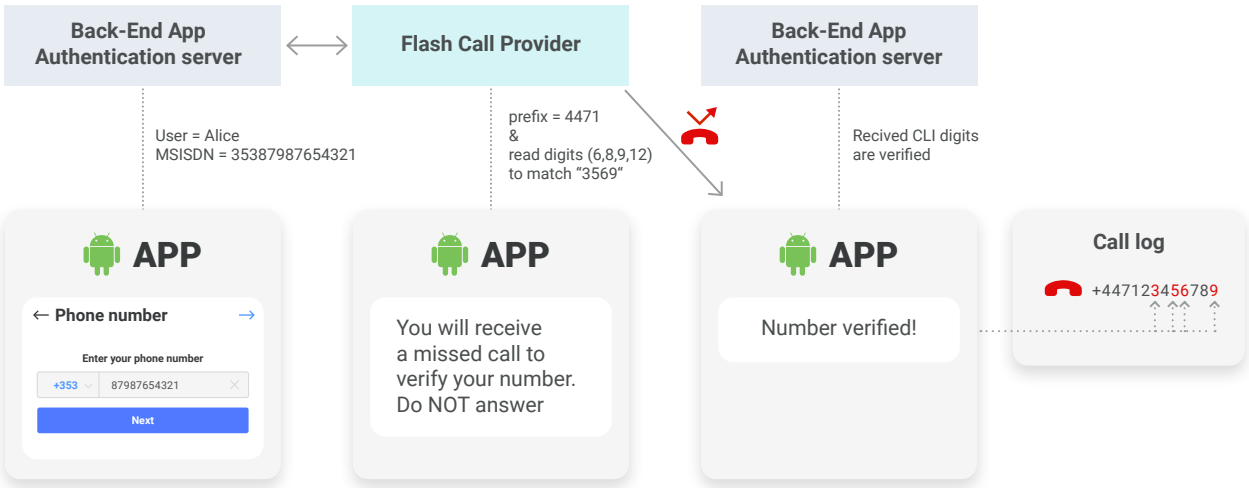
Flash Call emergence is not seen in markets where a single priced A2P product for domestic and international exists – this price is stable, predictable and without a history of increases.

[1] It is well established that price increase also results in more aggressive discovery of grey routes.

FLASH CALLS – HOW DO THEY WORK?

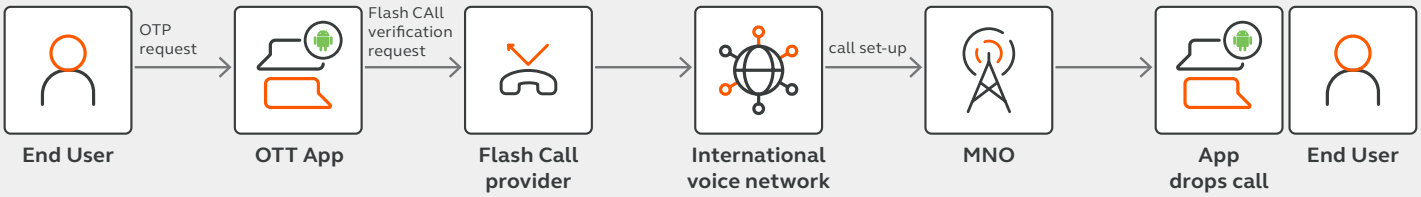
Flash Calling is the process in which a customer's phone number identity is verified via a phone call termination to that same number. In contrast to A2P SMS, the OTP digits are delivered as part of the "caller number", commonly referred to as the calling line identification (CLI). The authentication flow using Flash Calls is frictionless and in many cases the subscriber is not required to do anything manually, ensuring a good customer experience.

However, this method only works for smartphone apps that need to verify the MSISDN entered by the user. An app that supports Flash Call verification is instructed by its own back-end server to wait for a missed call matching a certain mask prefix. The app then drops the call and accesses the phone's missed call log to read the OTP digits from the CLI in the missed call log entry.



Note: this is just one method for how the OTP is selected from the CLI and verified.

The delivery of Flash Calls is usually operated by a provider, usually via APIs to companies that wish to use this method. The delivery of Flash Calls usually transits the international voice network and enters the MNO network (who owns the MSISDN subscription) via the associated international interconnect.



Flash Calls by default incur a zero-cost termination charge as they are essentially missed call events inside the mobile network. This allows Flash Calls to be more cost effective and priced at a cheaper rate than A2P SMS.

COMPARING FLASH CALLS TO A2P SMS

There are other criteria to compare Flash Calls with A2P SMS, apart from pricing. The three main ones are:

- Customer experience
- Quality
- Security

Customer experience:

Flash Calls offer a frictionless number verification method where the customer doesn't need to copy/paste the received OTP. One may argue that customers might be confused by the missed call entry in the call log or the icon on the notification bar, but all known apps counteract this by informing them about the impending missed call. However, customer consent is required during app installation to access the call log. This means the method only effectively works with android apps that offer telephony services[2]. The A2P SMS method can also support the same seamless verification step when the customer provides permission for the app to access their SMS inbox. Thus, allowing the app to auto-find the OTP in the A2P SMS message.

Quality:

A2P SMS is regarded as offering better quality, especially if is delivered on direct connect routes. Unless of course the A2P messaging providers attempt to deliver the OTP SMS via grey routes (which can result in blocking or severe obfuscation of the sender Id and the contextual text of the OTP communication). Flash Call would need direct voice connects to the MNO network (e.g., SIP interconnect between the MNO and the FC provider) to achieve the same quality. As it is, Flash Call delivery is occurring over the international voice network which can consist of many hops between the FC provider and the destination MNO network leading to quality issues on call termination. Furthermore, it is well known that the CLI can become manipulated (also known as "CLI refiling") or suppressed with multi-hop routing.

Security:

There are often claims that SMS is not secure. We know that (unlike most OTT messaging) there is no end-to-end encryption for SMS services (mainly as the MNOs are obliged to provide lawful intercept services). However, this same limitation applies to Flash Call as the CLI (which contains the sensitive OTP digits) is also not end-2-end encrypted. On further analysis, we can see that Flash Call has additional weaknesses when compared to A2P SMS:

[2] Apps offering telephony services, such as OTT apps, may request for customer permission to access the device call logs. Apps not offering telephony services will not usually request for such access.

Therefore, non-telephony related apps may not benefit from the seamless flash call user experience such as banking and e-commerce apps.

Fraud Type	Impact	A2P SMS	Flash Call
SIM Swap	Fraudsters can sign-in to an app on the swapped SIM and hijack the victims social media / OTT account.	!	!
Intercept	Fraudsters can use an SS7 vulnerability that allow SMS and voice termination calls to be redirected to their system.	!	!
Call Forwarding attack	Fraudsters can conduct an illegal call forwarding attack on a victim's MSISDN, so all calls are forwarded to a phone controlled by the attacker.	✕	!
Grey Route (revenue leakage)	Grey route threats emerge once an OTP delivery method is monetized by the MNO.	!	!
CLI Spoofing	Fraudsters conducting CLI spoofing attacks may offer Flash Call services and use spoofed CLIs.	✕	!
SIM Box	Fraudsters operating SIM Box or SIM Farm as grey route for SMS and voice, may also offer Flash Call services.	!	!

Flash Call delivers the OTP as part of the CLI metadata whereas OTP is delivered as part of the message text for A2P SMS. Thus, the OTP has better protection from unauthorized discovery in jurisdictions where SMS message content is protected by data privacy regulations.

Should an MNO wish to monetize Flash Call delivery, then there is an equal threat of them being delivered via grey routes (e.g., international interconnect, SIM box devices, etc.). Such grey routes can only be eliminated by an effective voice filtering solution, and with the creation of "white routes" via dedicated connections between MNOs and legitimate Flash Call providers.

WHY ARE FLASH CALLS A HOT TOPIC?

Based on the comparative analysis, we can conclude that the main reason for the recent emergence of Flash Calls is cost, due to the increasing price of international A2P SMS in certain regions beyond affordable limits for many enterprises. Enterprises need cost predictability and not escalating higher pricing for the same product – this is just not sustainable for any business.

Flash Calls are cheaper than A2P SMS in most markets as the MNO termination fee is currently zero-rated. It is often the case that zero-duration calls are not even generating CDRs for the MNO billing systems. It is hardly surprising that this OTP delivery method is emerging as another channel in “sweet spot” markets with high android smartphone penetration and A2P SMS costs.

AS AN MNO, WHAT CAN I DO?

MNOs need to strategically examine their value for the whole ecosystem of phone number (MSISDN) verification. In their favor, they provide the network assets that can be ubiquitously used on any device to implement the verification process in a secure and trusted manner.

If MNOs tactically decide to provide multiple channels for the phone number verification, then they need to consider the merit and use case for each channel and market this accordingly. For example, a text to speech call can be used in areas where the literacy rate is low. In the case of multiple channels, pricing needs to be designed such that the maximum revenue is gained overall. For example, one channel can be used as a secondary method in case of failure of the primary channel – meaning that the revenue associated with phone number verification is booked in case of failure on the primary channel. Price differentiation (if any) across different channels can often result in reduced revenues overall due to “channel churn”.

Therefore, MNOs should be careful designing the right pricing strategy for the current dominant international A2P SMS channel, first considering the threats and consequences that a high price brings, namely

- The continuing use of more aggressive grey routing on the SMS, SS7 and SIP channels using newly discovered vulnerabilities.
- The emergence of Flash Call delivery of OTPs over unmonetized voice signaling channels
- Emergence of alternate delivery channels that will completely bypass the MNO (e.g. WhatsApp Business messaging)

An existing international A2P SMS business needs to be sustained into the long-term future – we firmly believe that price stability and predictability is core to making this happen. In some cases, a downward price adjustment should be considered (which in theory should attract more volume).

It doesn’t matter if an MNO offers an omnichannel service for MSISDN or a purely SMS one – either way they need to protect their revenues. While most SMS Firewalls only protect text messages, in order to offer verification over multiple channels, MNOs need to plan and deploy an “omnichannel” firewall supporting SMS, Voice, Signaling and other native channels such as MMS and RCS.

Existing vendors or partners supplying A2P SMS monetization firewalls can also be assessed for upgrading to omnichannel support. An omnichannel firewall also has the advantage as it can correlate the shifting of white traffic onto grey routes that are using a different underlying channel. This is not possible via siloed multichannel firewalls.

CONCLUSION

After weighing up the pros and cons of Flash Calls, we don't consider Flash Calls will represent a significant new revenue stream for MNOs. However, they do clearly represent a revenue leakage threat especially if international A2P prices are incremented. In the case that MNOs decide to monetize Flash Calls, we believe that most of the revenue for this channel will initially churn from the A2P SMS line.

Our recommendations:

Phone Number Verification is a valuable service
Consider mobile phone number verification as a valuable product where MNOs are uniquely positioned to provide trusted network services for the enterprise market to enable phone number verification.

Pricing is critical
In the case of productizing this over multiple channels, the pricing policy needs to reflect the value (to the enterprise) of the overall phone number verification service and any channel differentiated pricing needs to be carefully set. The price needs to be predictable and sustainable for the enterprise client base.

All channels need to be secured
Finally, independent of whether phone number verification is offered over A2P SMS only or additional channels such as Flash Call, all channels (or bearers) which can deliver OTP digits to the device attached to the phone number need to be secured.

Investigate an omnichannel firewall
Full scope of required protection and real-time insights of monetized and emerging fraud traffic is best achieved with an omnichannel firewall.

The Infobip Advantage

GLOBAL REACH AND LOCAL PRESENCE

- 700+ direct-to-carrier connections
- Connect with over 7 billion people and things
- Strong enterprise client base
- 70+ offices on 6 continents

Our local presence enables us to react faster and have everyday interactions with our customers, providing solutions in line with their needs, local requirements and based on proven global best practices.

SCALABLE, FAST AND FLEXIBLE SOLUTIONS

- Best-in-class delivery rates
- High speed and reliability
- Low latency
- In-house developed platform

Our solutions are created to adapt to the constantly changing market and communication trends at speeds and levels of precision and personalization that only an in-house solution can offer.

REMARKABLE CUSTOMER EXPERIENCE

- Technical expertise
- Solutions and CX consultancy
- Customer success management
- 24/7 support and network monitoring

We will help you to get up and running in no time, whether it's assisting with integrations, messaging best practices or solutions consultancy

OWN INFRASTRUCTURE

- Locally available services
- Compliance to local regulations
- 40 data centers worldwide

Our worldwide infrastructure easily scales horizontally, leveraging the hybrid cloud model to never run out of resources. Our built-in global compliance engine is constantly updated with the latest in-country regulations and operator requirements.

Future Digital Awards — Recognising Challengers and Disruptors
JUNIPER RESEARCH

PLATINUM WINNER AS THE BEST SMS FIREWALL PROVIDER 2022
PLATINUM WINNER AS THE BEST CPAAS PROVIDER IN 2022 & 2021
PLATINUM WINNER AS THE BEST RCS PROVIDER IN 2021
PLATINUM AWARD AS THE GLOBAL CPAAS PROVIDER IN 2020
PLATINUM AWARD AS THE EMEA CPAAS PROVIDER IN THE 2020
PLATINUM AWARD AS THE BEST RCS PROVIDER IN 2020
GOLD AWARD AS THE BEST DIGITAL IDENTITY SOLUTION IN 2020

IDC — CPAAS LEADER IN IDC MARKETSCAPE 2021

THE PRODDY AWARDS — MESSAGING WINNER 2021
BEST CUSTOMER ENGAGEMENT PLATFORM 2020

ROCCO
BEST A2P SMS VENDOR AS RATED BY MNO'S 2017, 2018, 2019, 2020, 2021, 2022
BEST A2P SMS VENDOR AS RATED BY ENTERPRISES 2019, 2020, 2021
BEST SMS FIREWALL VENDOR AS RATED BY MNOS 2017, 2018, 2019/2020, 2021
TOP VENDOR INNOVATOR OF 2022

MEFFYS 21 WINNER — WINNER - COVID-19 FAQ CHATBOT OVER WHATSAPP

CC-GLOBAL AWARDS BERLIN 2020 — BEST GLOBAL SMS SERVICE PROVIDER - WHOLESALE SOLUTION 2020

MESSAGING & SMS GLOBAL AWARDS 2019
BEST OTT PARTNERSHIP 2019
BEST MESSAGING INNOVATION - BEST RCS IMPLEMENTATION 2019

4X AWARD WINNER 2018
BEST MESSAGING API
BEST MESSAGING INNOVATION-CARRIER SOLUTION
BEST ANTI - FRAUD INNOVATION
BEST SMS / A2P PROVIDER FOR THE EMEA REGION

TRUST IN ENTERPRISE MESSAGING
mobile connect
PCI DSS COMPLIANT — LEVEL 1 SERVICE PROVIDER
ISO 9001 ISO 27001 BUREAU VERITAS Certificatio
HIPAA COMPLIANT

www.infobip.com