Future of Messaging (FoM) Fraud & Revenue Assurance **Working Group**

- 14th of February 2024

MEF
FUTURE OF MESSAGING PROGRAMME

Anti-Trust Policy

- Anti-trust law prohibits agreements (written or implicit) between competitors that may negatively impact consumers or competitors and sharing of confidential information
- Anti-trust violations do not require proof of a formal agreement. A violation may be alleged based upon the mere appearance of unlawful activity.
- All meeting participants must abide by the following rules:
  - DO clearly identify the positive purpose of each project and follow it
  - DO NOT enter into agreements that restrict other parties' actions
  - DO NOT give rise to barriers to market entry
  - DO NOT discuss or exchange specific, confidential or commercially sensitive data on pricing, promotions and business plans
- Anti-trust laws do not prohibit petitioning the government, educating and informing the public, improving quality and safety standards, or protecting the public from fraud.

Your FoM Fraud & Revenue Assurance Working Group Team

- **Nick Rossman**
- Lead (interim) for Future of Messaging Programme

Director of Products

- **Ross Flynn**
- Project Manager

Project Manager

Working Group Administration

- If you would like to add your colleagues to this or any other working group then all you need to do is to email us at WG@mobileecosystemforum.com with all the details – name, email address and list of groups they would like to be added to

- Don’t forget that to be able to access all content MEF offers its members, including recordings of working group meetings and presentations shown at them, you need a MEF member log in. If you don’t have one of those, simply go to https://mobileecosystemforum.com/login/ and register. Only takes a couple of minutes. Your application will then be manually vetted and approved by our Global Member Manager Ewa Pepitt

FoM Fraud & Revenue Assurance Working Group

MISSION
To defend the long-term success of all Business Messaging channels, protecting customers and industry stakeholders from fraud and abuse, optimizing customer experience

DELIVERABLES

- Monthly forum for the review and discussions of new threats
- Whitepaper/reports/infographics/webinars/videos/social media to educate the market and stakeholders
- Creation of best practices for securing customer experience and revenue flows (FoM Best Practice)
- Aligning MNOs with pro-active approaches to managing the security and monetisation of Business Messaging

FOUNDING MEMBERS

- AdaptiveMobile
- Aegis Mobile
- ANAM Technologies
- BICS
- BT/EE
- Cellusys
- GMS
- Globe Teleservices (GTS)
- iBasis
- imimobile
- Infobip
- Intis Telecom
- iTouch Messaging
- LANCK Telecom
- Mobilesquared
- Nettzer
- Ooredoo
- Orange
- Route Mobile
- Sinch
- TATA Communications
- Telefonica
- TelQ
- Vox Solutions

Artificially Inflated Traffic

- 1) The lay of the land
  2) MEF initiatives 2022-23
     - ❖ Next Steps:
       - a) Improved Industry collaboration
       - b) Strengthening self-regulation and quality benchmark
       - c) Disseminating commercially available solutions
  3) Gap analysis
  4) Proof of concept
  5) Next steps

The Lay of the Land

Simeon Coney, ENEA Adaptive

ENEA

Artificially Inflated Traffic:
The need for clarity in definition

What is AIT?

GSMA

SMS traffic that is generated for the fraudulent purpose of generating revenue associated with its delivery for certain parties in the SMS traffic chain.

SMS AIT traffic is typically disproportionate to the overall amount of traffic that would be expected from a good faith usage or acceptable and reasonable commercial practice.

AIT characteristics include no motivation by the sender brand to communicate any content within the message to a recipient end user, and the motivation is typically for financial gain to one party at the unauthorized expense of one or more others.

i3Forum

Application to Person SMS
Artificial Inflation of Traffic (AIT), aka Artificial Generated Traffic (AGT), occurs when a party generates automated messages to fake, invalid or legitimate numbers with the intent to:

- Artificially force an originating Enterprise to send A2P SMS to a destination that is not a legitimate customer of that Enterprise or send A2P SMS not requested by a legitimate user of that Enterprise.
- Artificially force and defraud an originating Enterprise to pay a downstream vendor (SMS aggregator or MNO) to send the artificially generated traffic.

AIT contributes to the forced transfer and cascading of money from the sending Enterprise being defrauded to the downstream fraudster that artificially generated the traffic as they can control and collect the revenue of traffic to the destination numbers.

Person to Person SMS

- Artificially force an originating MNO Mobile subscriber to send P2P SMS to another MNO.
- Artificially force an originating MNO Mobile subscriber and its MNO to pay a downstream vendor (a P2P SMS aggregator and/or another MNO) for artificially generated P2P SMS traffic.

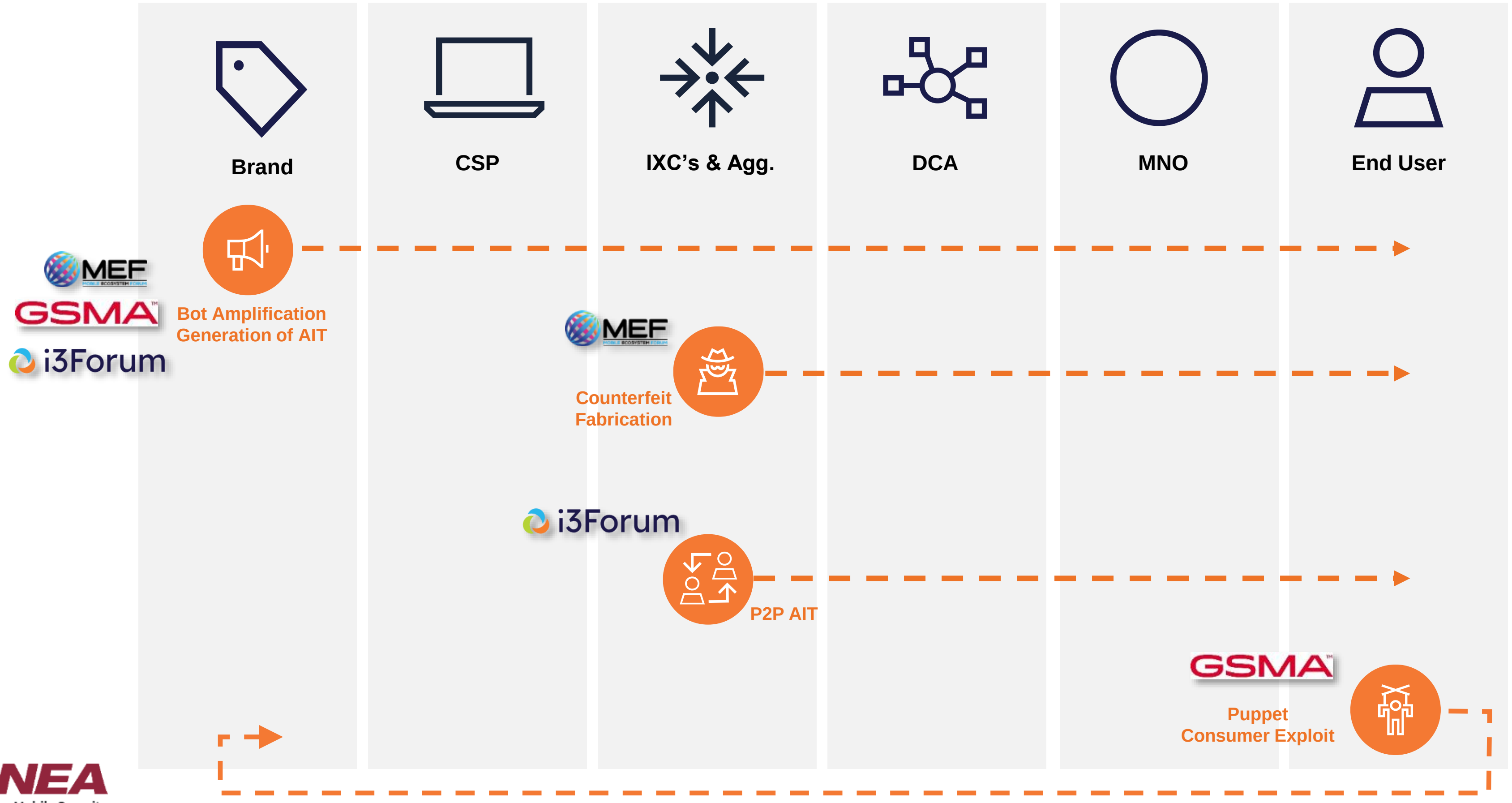
MEF MOBILE ECOSYSTEM FORUM

Two overarching types of Artificial Inflation of Traffic (AIT) fraud types.

The first is **defrauding a business**, by having bots in the guise of fake users send out one-time-password verification SMS via the business' messaging account to a number for which the fraudster is part of the SMS delivery chain. The fraudster makes a profit directly or indirectly from the messages at the business' expense.

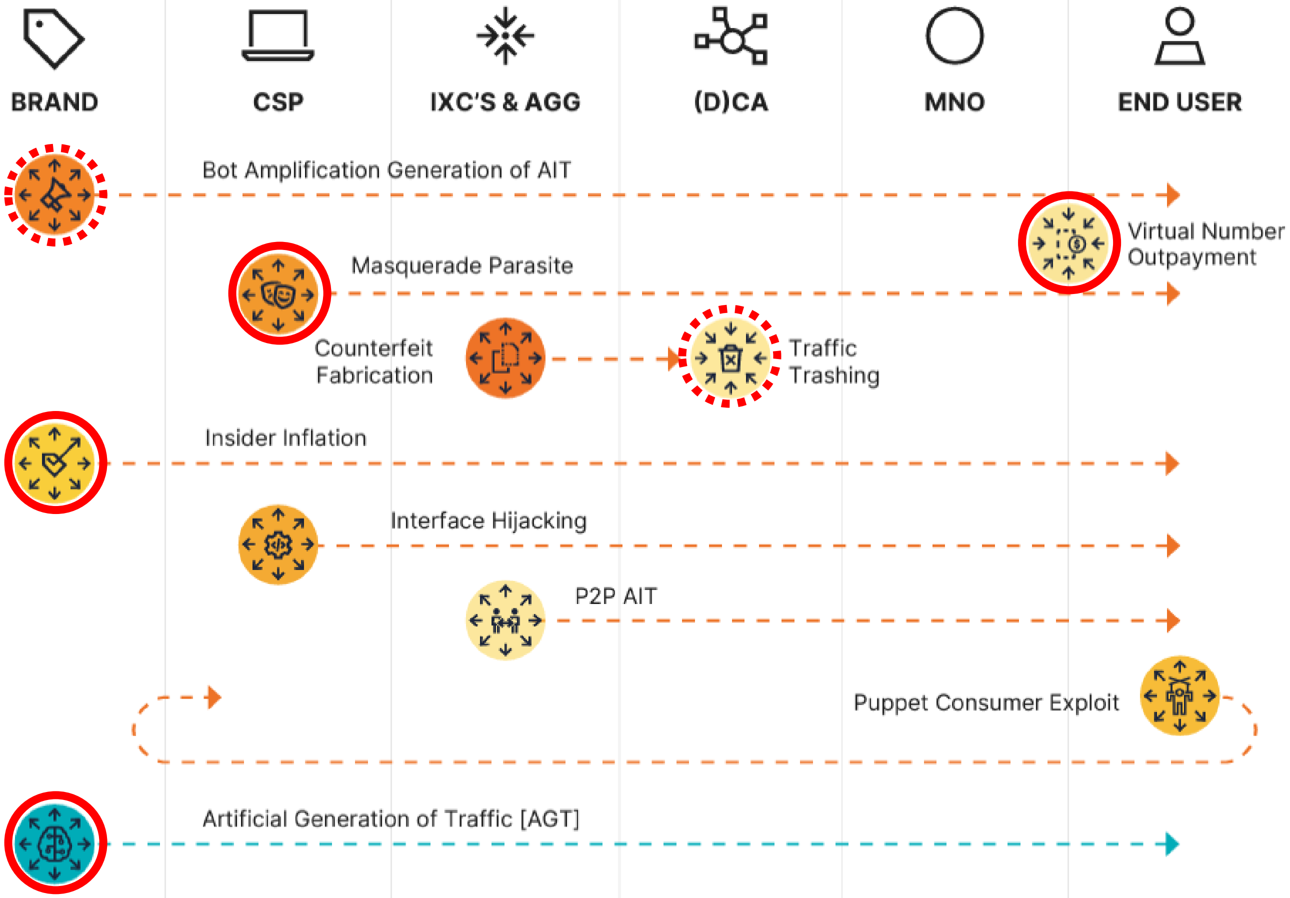
The second is **defrauding a mobile operator**, by generating messages sent to virtual numbers controlled by the fraudster that generate an outpayment. The fraudster makes a profit as the cost of sending the messages is lower than the outpayment

Is the AIT Issue Well Understood?



ENEA
AdaptiveMobile Security

Enhancing the Definitions



ENEA
AdaptiveMobile Security

Defining the Main AIT Types

Counterfeit Fabrication AIT

1

Traffic is generated “in transit” by one of the aggregators in the chain and is not visible at that point in the flow, or by any other aggregators who may be terminating traffic to the same destinations. It is a deliberate action by the generating aggregator to generate fake traffic impersonating that of a brand, hence the counterfeiting association.

Amplification Bot Generation of AIT

2

This fraudulent attack generates synthetic traffic at the brand by exploiting fake accounts within the service, or unprotected service interfaces. It is difficult to control (with low false positives) across the message ecosystem as originating intelligence is not available (eg account ID, IP address used etc). The purpose of this AIT attack is to generate traffic from within the brand’s service that passes through the full chain, typically generating revenue for each stage in the chain, at the cost

Masquerade Parasite Generation of AIT

3

The purpose of this AIT attack is similar to those described above but differs as the brand or “aggregator partner” accounts are created at the CPaaS provider. These attacks have the express purpose of generating artificial traffic associated with brands that the account has no responsibility for, potentially blending the fake traffic with legitimate traffic, which has most likely been acquired through an existing aggregator relationship.

Interface Hijacking AIT

4

This AIT fraud attack compromises the API’s into the CSP and is used to generate fraudulent traffic. As with Counterfeit Fabrication AIT, the purpose of this attack technique is to generate additional traffic. The difference between this attack and the alternative techniques identified above, is that the CSP is compromised and not the brand.

Puppet Consumer Exploit for AIT

5

One method of generating traffic for the purpose of AIT is by having mobile operator subscribers generate the traffic unknowingly or unwittingly. There are a number of techniques to achieve this: malware, SMS apps, device hacking, and social engineering via SMS URI and SMS Wangiri.

Insider Inflation AIT

6

Artificial traffic is deliberately generated by the brand to inflate the number of active transactions or active users within the brand. It may be done using a range of techniques, such as bots or via brand API potentially making this fraud distinguishable from legitimate scenarios.

Addressing AIT

1 | Definition

2 | Measurement

3 | Solution availability

4 | Best practices agreement

5 | Gap identification

ENEA

www.Enea.com

MEF Activities

Dario Betti, MEF

MEF Activities (socialization)

Awareness & Alignment:

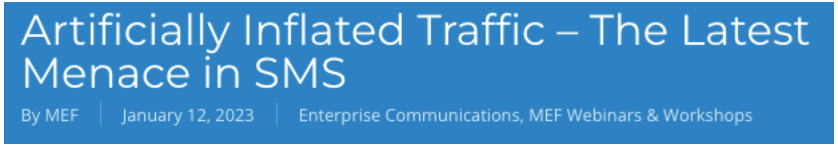
Blogs

Webinars

Events

Closed-Door session

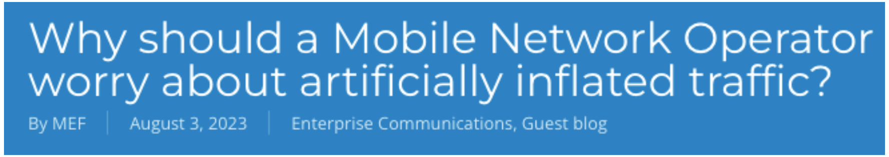
Reports



Artificially Inflated Traffic – The Latest Menace in SMS

By MEF | January 12, 2023 | Enterprise Communications, MEF Webinars & Workshops

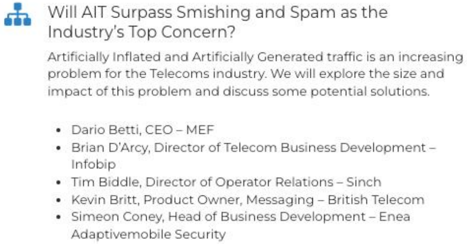
LINK: Uku Tomikas



Why should a Mobile Network Operator worry about artificially inflated traffic?

By MEF | August 3, 2023 | Enterprise Communications, Guest blog

LINK: Joanna Kuligowska, HAUD



Will AIT Surpass Smishing and Spam as the Industry's Top Concern?

Artificially Inflated and Artificially Generated traffic is an increasing problem for the Telecoms industry. We will explore the size and impact of this problem and discuss some potential solutions.

- Dario Betti, CEO – MEF
- Brian D'Arcy, Director of Telecom Business Development – Infobip
- Tim Biddle, Director of Operator Relations – Sinch
- Kevin Britt, Product Owner, Messaging – British Telecom
- Simeon Coney, Head of Business Development – Enea Adaptivemobile Security

MEF WEBINAR

ARTIFICIAL INFLATION OF TRAFFIC (AIT) – THE BOT ARMY IS HERE AND THE BATTLE IS ON!

MARCH 23RD 2023
15:00 (UK TIME)

SUPPORTED BY VOX SOLUTIONS

MEF Activities (Report)

White Paper – Safeguarding the long-term future of international SMS* :

- White paper (to be published shortly) in conjunction with:

sinch

routemobile
communication simplified

infobip

Mobilesquared
Decision ready data

GMS GLOBAL MESSAGE SERVICES

bics

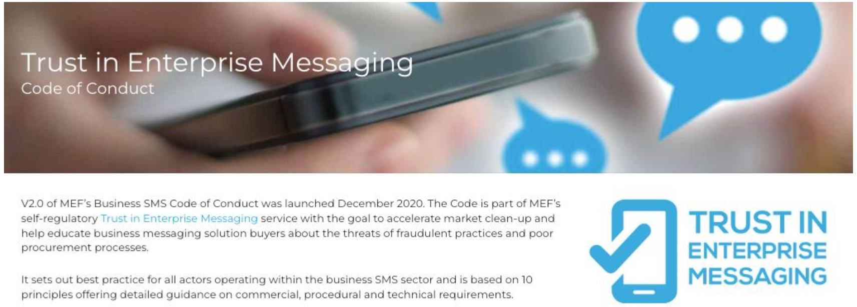
monty mobile
THE ART OF TELECOM

*Tentative title

MEF Activities (Code of Conduct)

MEF Code of Conduct:

- Currently 53 signatories
- Encourage more members to sign code of conduct
- Beef up:
  - Section addressing AIT
  - Monitoring process
  - Enforcement:
    - Members only do business with signatories?
    - Penalties?
    - Dispute mechanism?



Trust in Enterprise Messaging

Code of Conduct

V2.0 of MEF's Business SMS Code of Conduct was launched December 2020. The Code is part of MEF's self-regulatory Trust in Enterprise Messaging service with the goal to accelerate market clean-up and help educate business messaging solution buyers about the threats of fraudulent practices and poor procurement processes.

It sets out best practice for all actors operating within the business SMS sector and is based on 10 principles offering detailed guidance on commercial, procedural and technical requirements.

TRUST IN ENTERPRISE MESSAGING

[LINK]

MEF Activities - Messaging

In summary, the message is:

1) Better Industry Collaboration:
   a. Exchange of non-confidential data – "centralized" database
   b. Track flow of traffic
   c. Global standards (brand identity)
2) Better ways to combat AIT fraud
   a. Adapt existing solutions
   b. New solutions to address gaps
3) Socialization:
   a. Continue educating the ecosystem, including regulators, brands, MNO's and aggregators

Produce a comprehensive list of companies that offer AIT anti-fraud solutions and potentially add it to the MEF website, such as:

- BICS
- Telesign
- Vox Solutions
- Lanck Telecom
- GTS
- Sinch
- Twilio
- Haud
- AB Handshake

Breakdown of solutions by those aimed at:

✓ Enterprises
✓ Operators
✓ Aggregators

Solutions Showcase

List of proposed and existing anti AIT fraud solutions

AB Handshake

Dmitry Sumin

AB HANDSHAKE`S EXPERTISE

AB HANDSHAKE IS A GLOBAL PROVIDER OF TELECOM FRAUD PREVENTION SOLUTIONS FOR OPERATORS AND ENTERPRISES

160+
Operators protected worldwide

4.5 MLN
SMS AIT identified monthly

2+ MLN
Fraud call attempts blocked daily

CONTRIBUTING TO:

GSMA™

GSMA Telecommunication ISAC

ITU ASSOCIATE

CFCA

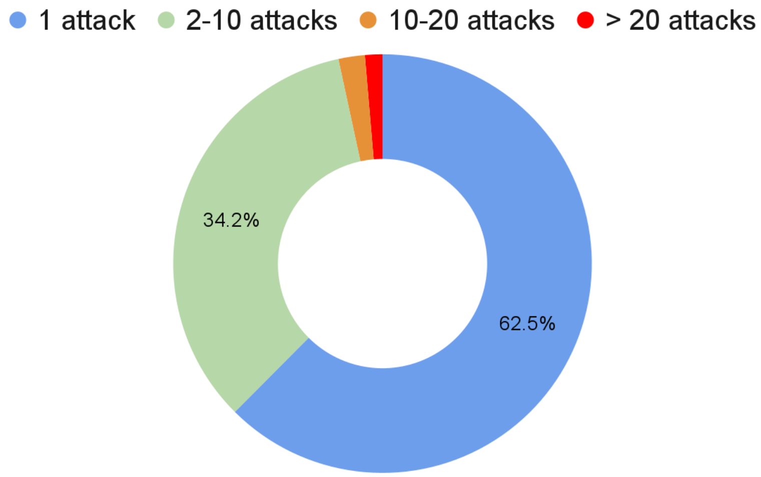
REPEATED NUMBERS IN ATTACKS

AB HANDSHAKE`S RECENT STUDY:

Total analyzed records between November 2022 and April 2023 - **19,222** (attacks not individual calls).

- **One attack** per single unique fraudulent number range shown in **62.5%** (12,005) of records.
- **34.2%** (6,566) used for between **2 and 10 attacks.**
- **2.0%** (392) used in **10 to 20 attacks.**
- **1.3%** (259) used in **20 or more attacks.**

Diagram: Percentage for numbers participating in multiple attacks



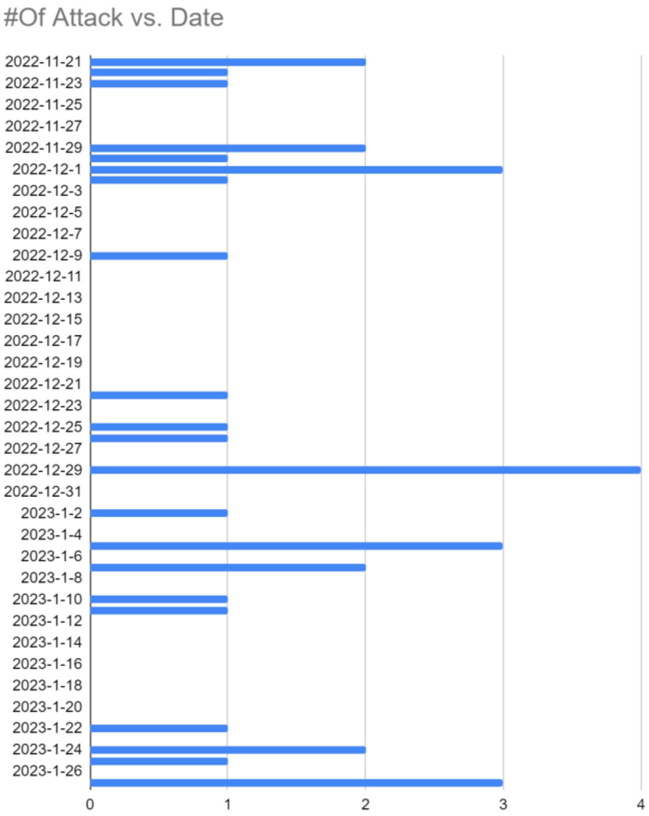
DIFFERENT CASE STUDIES

Case study #1. Belgium country code

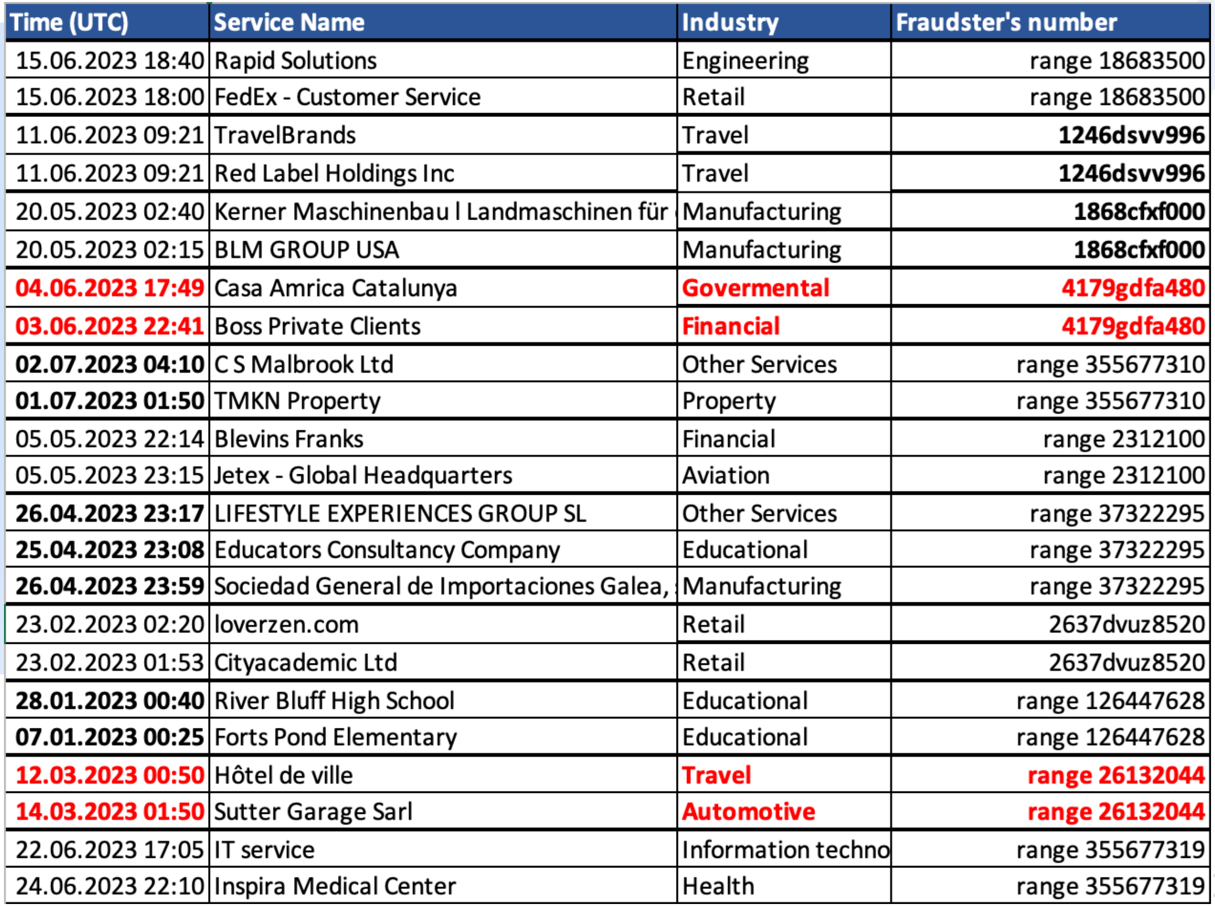
Range of numbers **32480338** was involved in **39** fraudulent attacks between January 21 and February 27, 2023.

Case study #2. Zimbabwe country code

Number range **26377** was involved in **34** fraudulent attacks between November 21 and January 27, 2023.

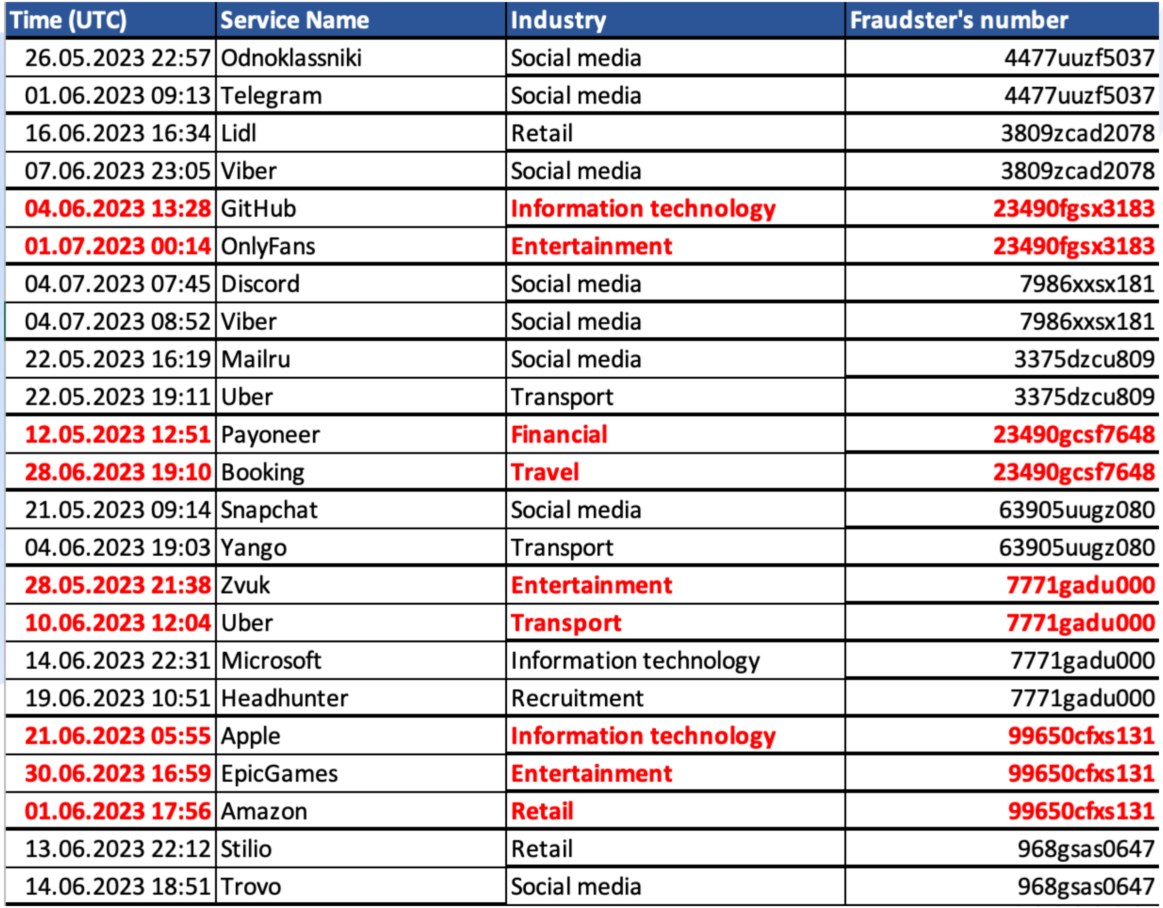


VOICE ATTACKS



Time (UTC)	Service Name	Industry	Fraudster's number
15.06.2023 18:40	Rapid Solutions	Engineering	range 18683500
15.06.2023 18:00	FedEx - Customer Service	Retail	range 18683500
11.06.2023 09:21	TravelBrands	Travel	**1246dsvv996**
11.06.2023 09:21	Red Label Holdings Inc	Travel	**1246dsvv996**
20.05.2023 02:40	Kerner Maschinenbau | Landmaschinen für	Manufacturing	**1868cfxf000**
20.05.2023 02:15	BLM GROUP USA	Manufacturing	**1868cfxf000**
04.06.2023 17:49	Casa Amrica Catalunya	**Govermental**	**4179gdfa480**
03.06.2023 22:41	Boss Private Clients	**Financial**	**4179gdfa480**
02.07.2023 04:10	C S Malbrook Ltd	Other Services	range 355677310
01.07.2023 01:50	TMKN Property	Property	range 355677310
05.05.2023 22:14	Blevins Franks	Financial	range 2312100
05.05.2023 23:15	Jetex - Global Headquarters	Aviation	range 2312100
26.04.2023 23:17	LIFESTYLE EXPERIENCES GROUP SL	Other Services	range 37322295
25.04.2023 23:08	Educators Consultancy Company	Educational	range 37322295
26.04.2023 23:59	Sociedad General de Importaciones Galea,	Manufacturing	range 37322295
23.02.2023 02:20	loverzen.com	Retail	2637dvuz8520
23.02.2023 01:53	Cityacademic Ltd	Retail	2637dvuz8520
28.01.2023 00:40	River Bluff High School	Educational	range 126447628
07.01.2023 00:25	Forts Pond Elementary	Educational	range 126447628
12.03.2023 00:50	Hôtel de ville	**Travel**	**range 26132044**
14.03.2023 01:50	Sutter Garage Sarl	**Automotive**	**range 26132044**
22.06.2023 17:05	IT service	Information techno	range 355677319
24.06.2023 22:10	Inspira Medical Center	Health	range 355677319

SMS AIT ATTACKS



Time (UTC)	Service Name	Industry	Fraudster's number
26.05.2023 22:57	Odnoklassniki	Social media	4477uuzf5037
01.06.2023 09:13	Telegram	Social media	4477uuzf5037
16.06.2023 16:34	Lidl	Retail	3809zcad2078
07.06.2023 23:05	Viber	Social media	3809zcad2078
04.06.2023 13:28	GitHub	**Information technology**	**23490fgsx3183**
01.07.2023 00:14	OnlyFans	**Entertainment**	**23490fgsx3183**
04.07.2023 07:45	Discord	Social media	7986xxsx181
04.07.2023 08:52	Viber	Social media	7986xxsx181
22.05.2023 16:19	Mailru	Social media	3375dzcu809
22.05.2023 19:11	Uber	Transport	3375dzcu809
12.05.2023 12:51	Payoneer	**Financial**	**23490gcsf7648**
28.06.2023 19:10	Booking	**Travel**	**23490gcsf7648**
21.05.2023 09:14	Snapchat	Social media	63905uugz080
04.06.2023 19:03	Yango	Transport	63905uugz080
28.05.2023 21:38	Zvuk	**Entertainment**	**7771gadu000**
10.06.2023 12:04	Uber	**Transport**	**7771gadu000**
14.06.2023 22:31	Microsoft	Information technology	7771gadu000
19.06.2023 10:51	Headhunter	Recruitment	7771gadu000
21.06.2023 05:55	Apple	**Information technology**	**99650cfxs131**
30.06.2023 16:59	EpicGames	**Entertainment**	**99650cfxs131**
01.06.2023 17:56	Amazon	**Retail**	**99650cfxs131**
13.06.2023 22:12	Stilio	Retail	968gsas0647
14.06.2023 18:51	Trovo	Social media	968gsas0647

AB HANDSHAKE PROPOSAL

SMS AIT fraud awareness sharing database:

- Timestamp
- Sender ID
- Terminating number range
- ...

Smishing attack awareness sharing database:

- Timestamp
- Sender ID
- Terminating number range
- Link / domain
- Text (description)
- ...

Console Connect

Carlos Dasilva

consoleconnect

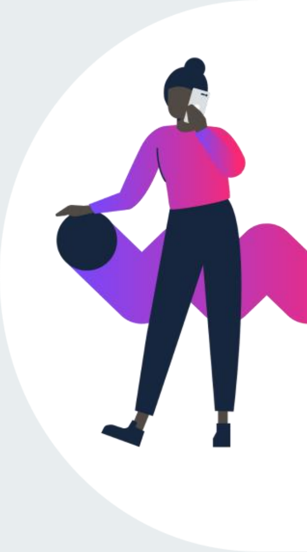
February 2024

MEF - AIT mitigation enforcement

Carlos DaSilva

AIT or **not AIT** ?

Sender ID	Content	Destination number	Could it be AIT ?
22000	G-354124 is your Google verification code	+12423224444	Maybe, Abnormal volume of OTP SMS towards a fix number
22000	G-765165 is your Google verification code	+12424342844	Maybe Abnormal volume of OTP SMS towards a mobile number suspected to be a SIMbox
22000	G-765163 is your Google verification code	+12424659955	**No way to be sure,** It's a real mobile user number
22000	G-765168 is your Google verification code	+12424342877	SMS was **trashed** by an aggregator, MNO never received it



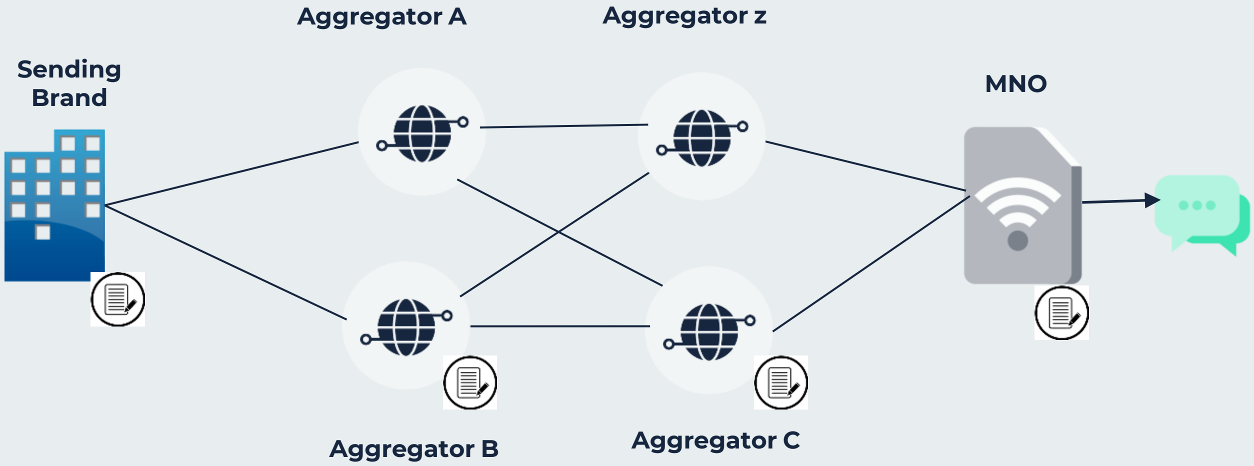
It is **impossible to substantially mitigate AIT** traffic by accurately **blocking it**.

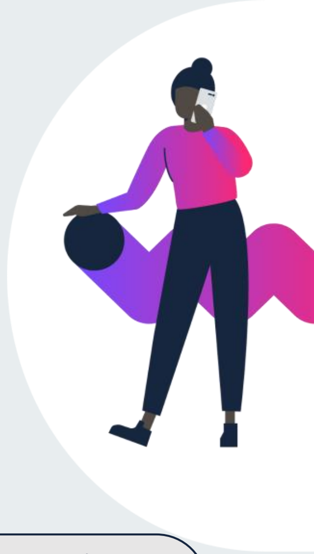
The proof is in the volumes

Despite many commercial solutions and industry education, AIT has been increasing at fast pace over the years, and nothing seems to be able to put a real dent to the growth of AIT.

How do we put down a fire: **remove oxygen**
How can we put down AIT: **remove the cash**

Economic good behavior incentive
The sender that signs the code of conduct
commits to select (when available) full routes/providers that have signed the code of conduct





Code of Conduct (could) state that **if AIT fraud is suspected, the portion of traffic that is suspected to be AIT, is not paid** to the downstream provider and is also not invoiced to the upstream sender

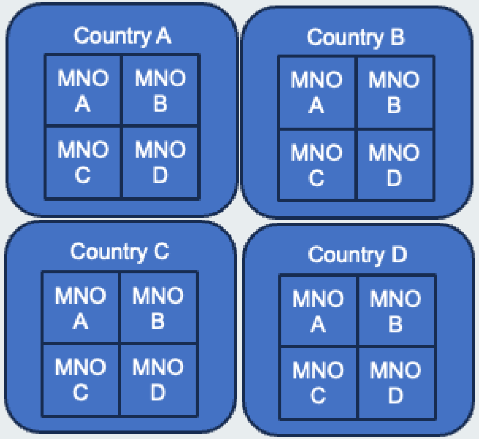
The suspicion of AIT fraud and (frozen) volume of AIT traffic is:

- the delta with **the reference given by a up-to-date market reference** for normal SMS/subscriber for other networks in the same country or SMS/subscriber in neighboring countries previous quarter
- Or **an arbitrary SMS/subscriber for a group of brands** for a country destination agreed between signatories ahead of time and actualized by an industry body on a quarterly basis

Use shared and trusted patterns from an industry crowd sourced database to identify AIT volumes

consoleconnect

(no need to know which SMS are AIT to block them)



Country A

MNO A	MNO B
MNO C	MNO D

Country B

MNO A	MNO B
MNO C	MNO D

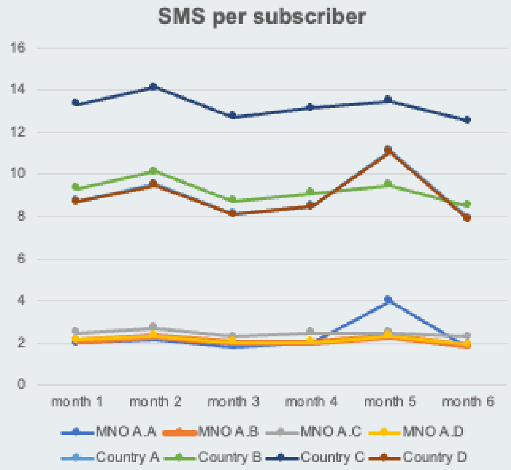
Country C

MNO A	MNO B
MNO C	MNO D

Country D

MNO A	MNO B
MNO C	MNO D

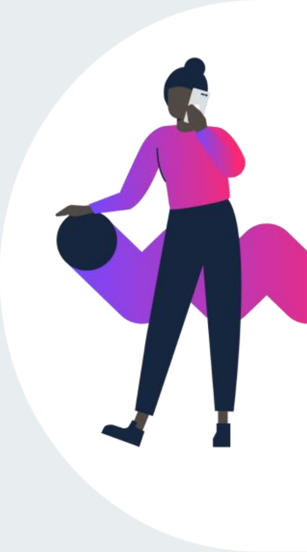
SMS per subscriber is a normalized and effective solution to compare networks, countries, regions



⚠1 Highly different upward increase may indicate AIT at the country level

⚠2 Highly different upward increase may indicate AIT at the MNO level

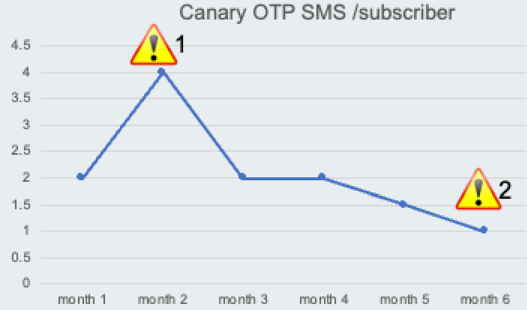
⚠3 Constant upward higher volumes may indicate AIT at the country level



Use shared and trusted patterns to identify AIT volumes

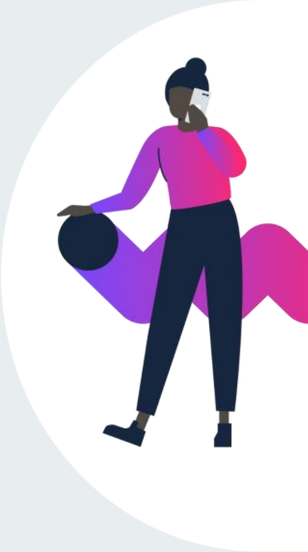
Over than 90% of the International A2P market is made of 20 brands that send SMS OTP.

The canary tracker in Insight is a group of representative A2P brands, anonymized as a total combined volume, and used to track, compare and analyze International market traffic trending



⚠1 Possible artificial traffic

⚠2 Possible Loss of SMS OTP , market substitution



The **end**

Telesign

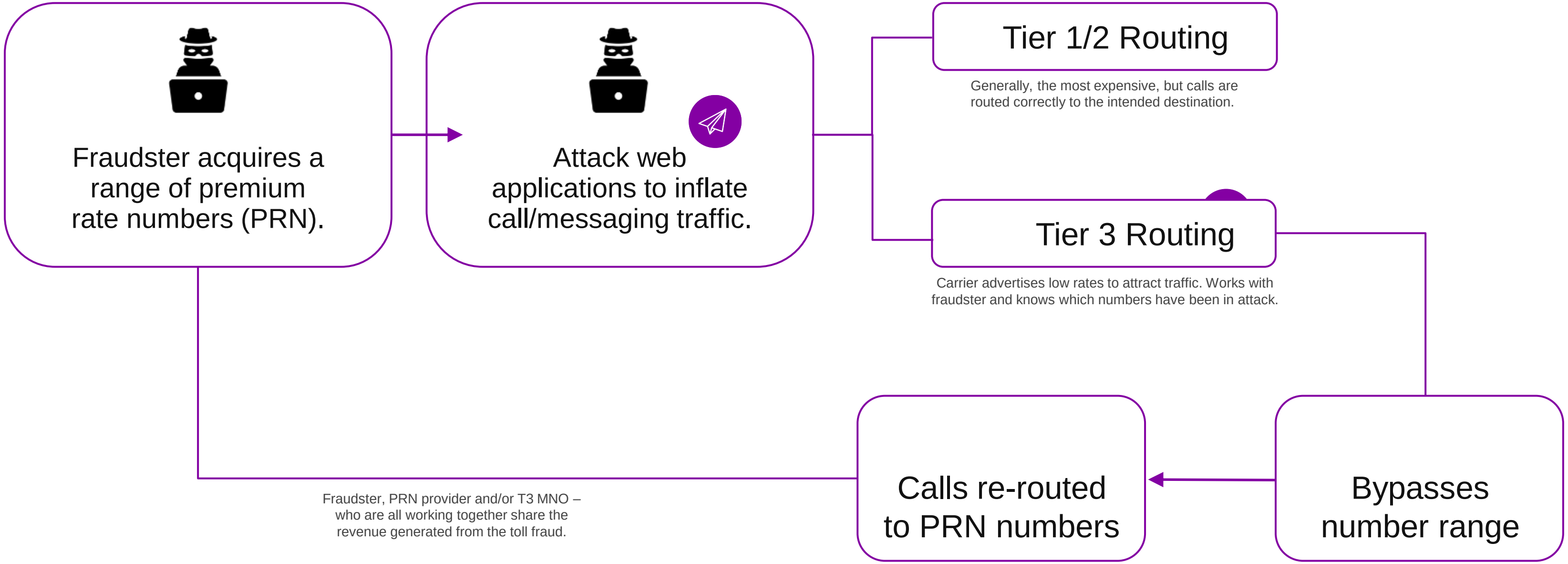
Shannon Donohue

Artificially Inflated Traffic prevention

Assess the risk of a phone number before inbound and outbound engagement.

Learn how

How Fraudsters artificially inflate traffic



Fraudster acquires a range of premium rate numbers (PRN).

Attack web applications to inflate call/messaging traffic.

Tier 1/2 Routing

Generally, the most expensive, but calls are routed correctly to the intended destination.

Tier 3 Routing

Carrier advertises low rates to attract traffic. Works with fraudster and knows which numbers have been in attack.

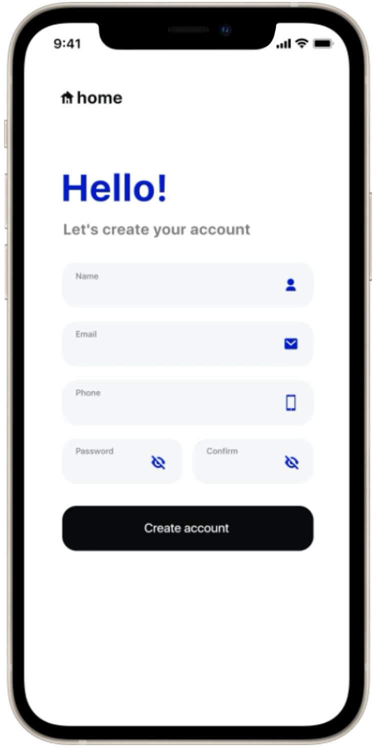
Bypasses number range

Calls re-routed to PRN numbers

Fraudster, PRN provider and/or T3 MNO – who are all working together share the revenue generated from the toll fraud.

Fraudster Acquires a Range of Numbers

291-315-5804
291-315-5805
291-315-5806
291-315-5807
291-315-5808
291-315-5809
291-315-5810
291-315-5811
291-315-5812
291-315-5813
291-315-5814
291-315-5815
291-315-5816
291-315-5817
291-315-5818
291-315-5819
291-315-5820



9:41

home

Hello!

Let's create your account

Name

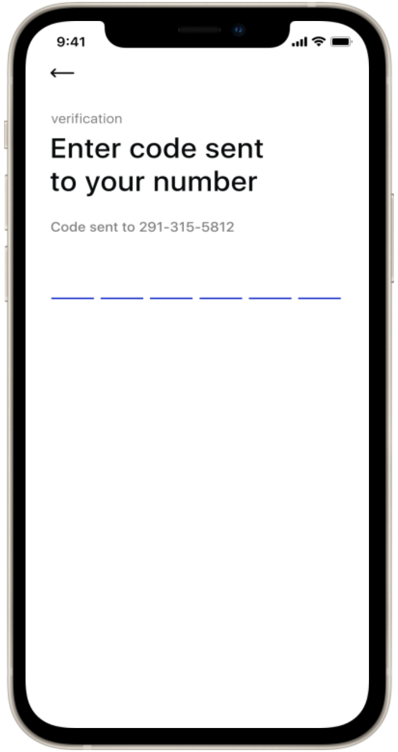
Email

Phone

Password

Confirm

Create account



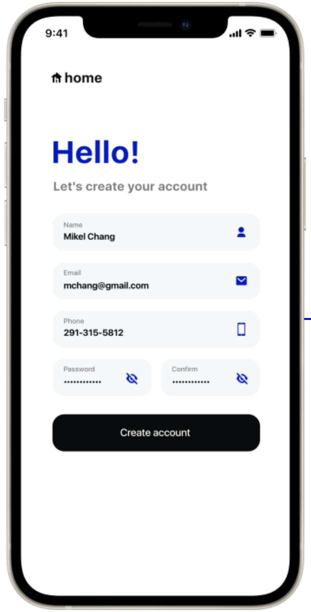
9:41

←

verification

Enter code sent to your number

Code sent to 291-315-5812



9:41

home

Hello!

Let's create your account

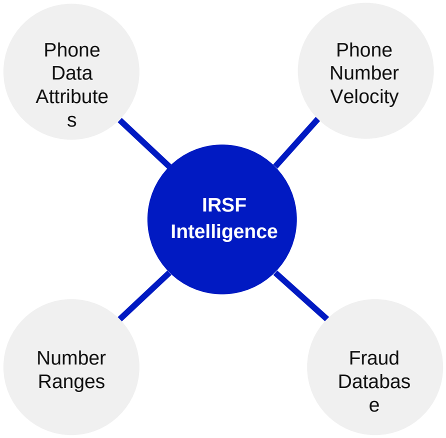
Name
Mikel Chang

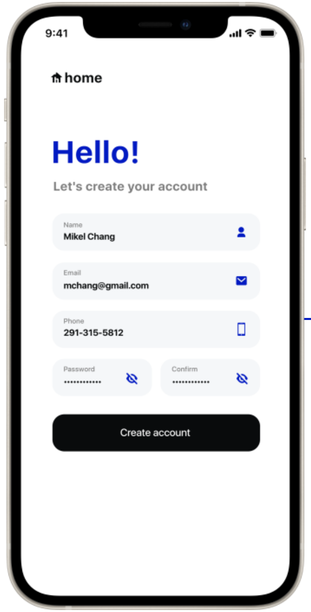
Email
mchang@gmail.com

Phone
291-315-5812

Password
••••••••••••

Confirm
••••••••••••





9:41

home

Hello!

Let's create your account

Name
Mikel Chang

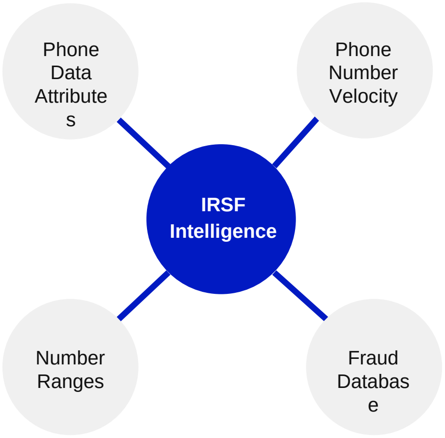
Email
mchang@gmail.com

Phone
291-315-5812

Password
••••••••••••

Confirm
••••••••••••

Create account



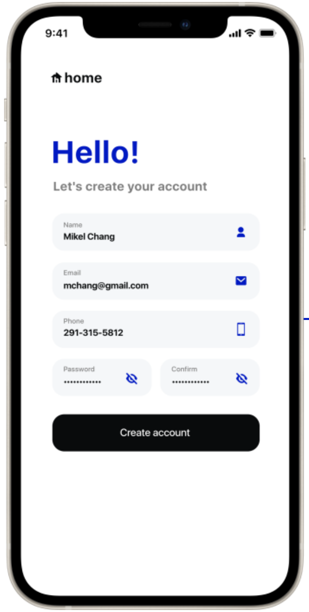
Phone Data Attributes

Phone type
Mobile, fixed line, non-fixed VOIP, toll-free, premium rate, invalid etc.

Carrier
Verizon, AT&T, Orange, O2, Jio, NTT, Vodafone etc.

Block listed
True or False

Run Trust Assessment



9:41

home

Hello!

Let's create your account

Name
Mikel Chang

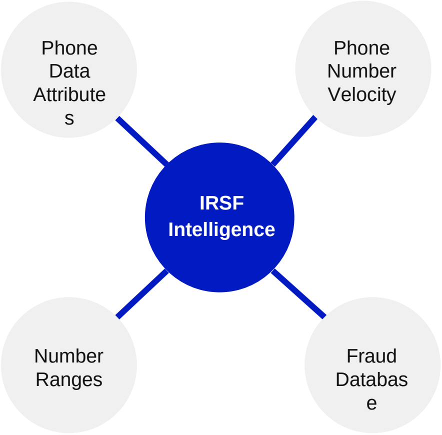
Email
mchang@gmail.com

Phone
291-315-5812

Password
••••••••••••

Confirm
••••••••••••

Create account



Phone
Data
Attribute
s

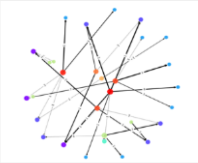
Phone
Number
Velocity

IRSF
Intelligence

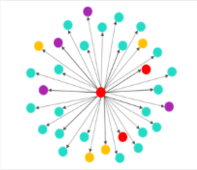
Number
Ranges

Fraud
Databas
e

Number Velocity



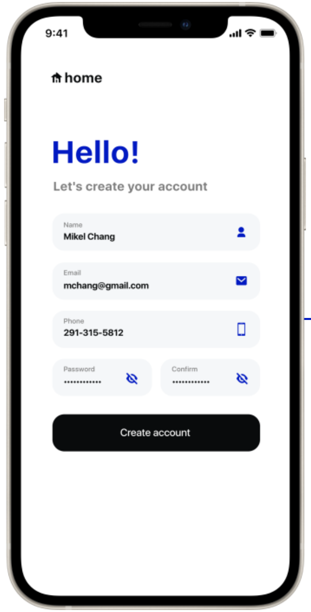
Human
Regular short-and long-term A2P traffic patterns.



Bot-behavior
Abnormal high volume of A2P and verification traffic.

Carrier
Assessment of carrier-specific traffic patterns.

Run Trust Assessment



9:41

home

Hello!

Let's create your account

Name
Mikel Chang

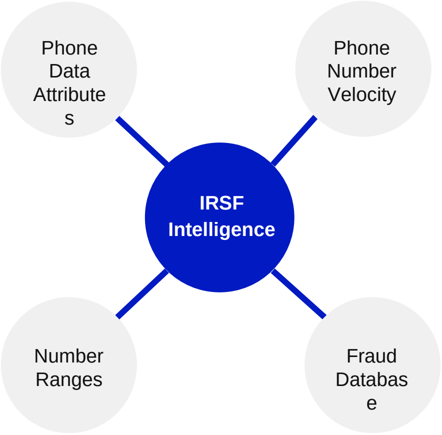
Email
mchang@gmail.com

Phone
291-315-5812

Password
············

Confirm
············

Create account



Phone
Data
Attribute
s

Phone
Number
Velocity

IRSF
Intelligence

Number
Ranges

Fraud
Databas
e

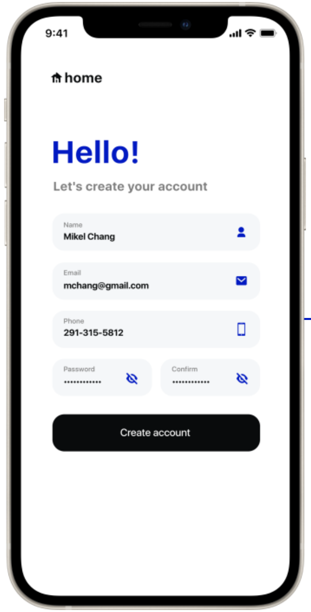
Fraud Database

Benchmark against Telesign's proprietary fraud consortium

2B+ Unique Phone Numbers

14 Of the largest web properties contribute

Run Trust Assessment



9:41

home

Hello!

Let's create your account

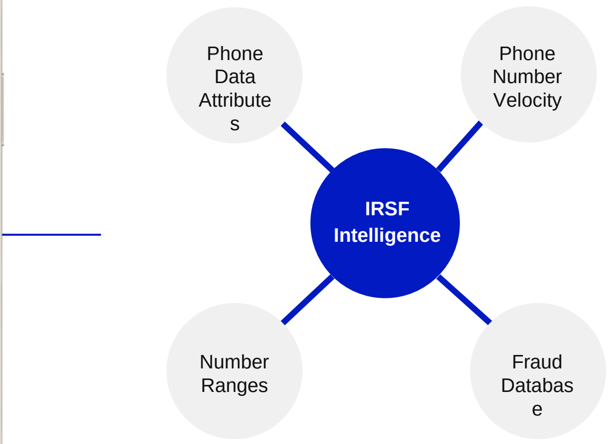
Name: Mikel Chang

Email: mchang@gmail.com

Phone: 291-315-5812

Password: ············

Confirm: ············



IRSF Intelligence

Phone Data Attribute s

Phone Number Velocity

Number Ranges

Fraud Databas e

Number Ranges

Number Range Risk Signals

Unassigned Numbers

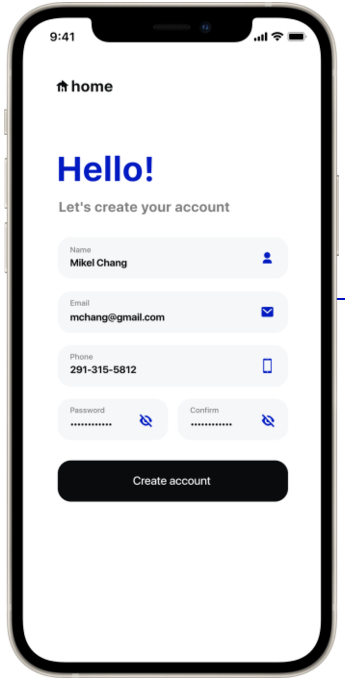
Short Time Intervals

Risky Countries

Premium Rate Numbers

291-315-5804
291-315-5805
291-315-5806
291-315-5807
291-315-5808
291-315-5809
291-315-5810
291-315-5811
291-315-5812
291-315-5813
291-315-5814
291-315-5815
291-315-5816
291-315-5817
291-315-5818
291-315-5819
291-315-5820

Run Trust Assessment



home

Hello!

Let's create your account

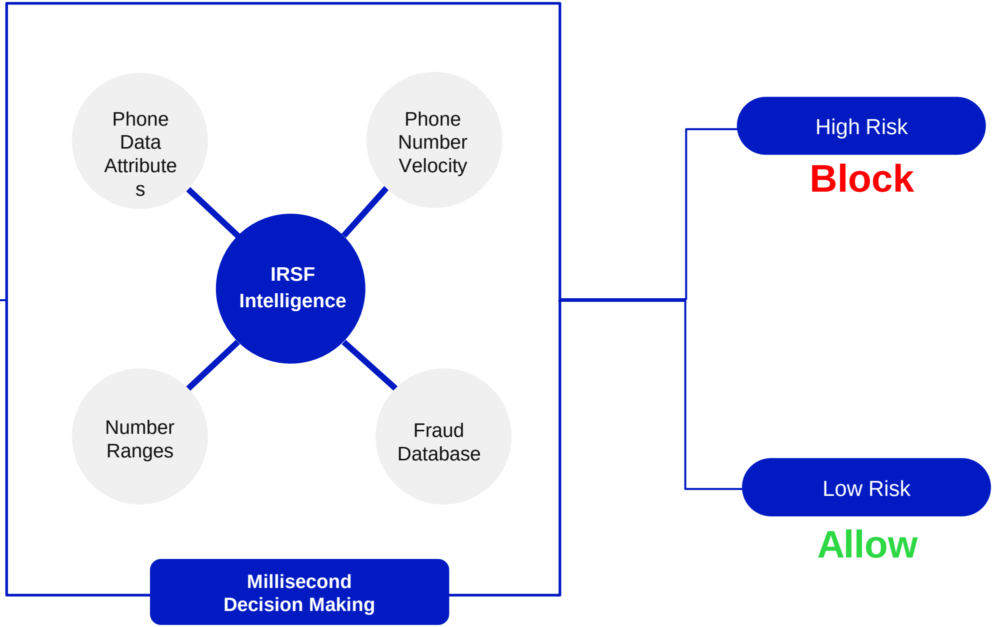
Name
Mikel Chang

Email
mchang@gmail.com

Phone
291-315-5812

Password
••••••••••••

Confirm
••••••••••••



Phone Data Attribute s

Phone Number Velocity

IRSF Intelligence

Number Ranges

Fraud Database

Millisecond Decision Making

High Risk

Block

Low Risk

Allow

Vox Solutions

Teodor Magureanu & Ehsan Ahmadi

Sinch

Mykhailo Odarchenko

AIT Detection and Mitigation

How do you detect AIT?

Sudden increase of traffic into new destination

Unlikely geographical destination for the customer to send SMS to

Destination numbers in sequential or nearly seque ntial order:

441234567890
441234567891
441234567892

Monitor conversion rate

AIT is an issue for the entire messaging ecosystem threatening operators, SMS providers, and brands.

AIT Detection and Mitigation

What we can do to stop AIT

Technical:	Commercial:
• Implementing AIT Detection and Prevention Systems • Proactively blocking high-risk AIT destinations • Setting volume limits towards high-risk AIT destinations	Creating industry accepted process for handling AIT: • Dispute handling • Payment blocking • Routing improvement • Closing coverage towards ”AIT destinations”

Twillio

Mike Piccirilli

SMS Traffic Pumping Protection Products & Features

SMS Traffic Pumping Prevention Products

Programmable Messaging

SMS Pumping Protection

Automatically detects and blocks SMS pumping with the Programmable Messaging API.

- Built into Programmable Messaging for customers with OTP use cases who do not want to or cannot migrate to Verify
- Can be used for multiple messaging use cases
- Effectiveness:
  - FP Rate: 0.5%
  - Block Rate: ~95% of fraud

Lookup

Lookup SMS Pumping Risk Score

Checks a phone number for known or suspected SMS pumping schemes with the Lookup API.

- Provides raw intelligence including Fraud Guard data on current or recent blocks
- User controls when to block traffic depending on their risk tolerance
- Can be used across providers for multi-sourcing customers
- Effectiveness:
  - FP Rate: 0.1% - 2% (user defined)
  - Block Rate: 85-95% of fraud

Verify

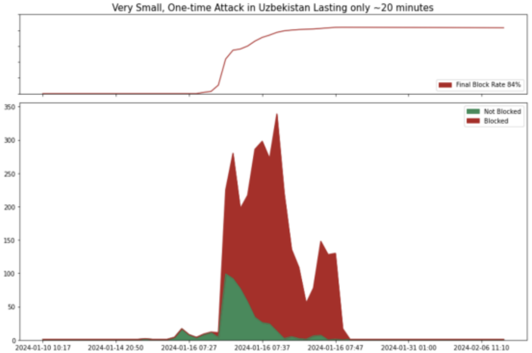
Verify Fraud Guard

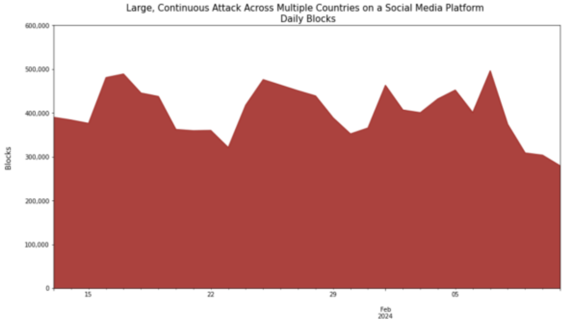
Automatically detects and blocks SMS pumping for OTPs with the Verify API.

- Highest efficacy of blocking SMS pumping with lowest false positive rate
- User customization of risk tolerance level (3 modes)
- Tailored to OTPs
- Effectiveness:
  - Basic: ~90% Block Rate, 0.1% FP Rate
  - Standard: ~95% Block Rate, <1.0% FP Rate
  - Max: ~98% Block Rate, <2.0% FP Rate

Features & signals based on: destination country, carriers, providers & aggregators, prefixes, and individual phone numbers

“The Party’s Over”


Very Small, One-time Attack in Uzbekistan Lasting only ~20 minutes


Large, Continuous Attack Across Multiple Countries on a Social Media Platform
Daily Blocks

Customer Value

Twilio has consistently been blocking between 1.5M - 2.5M fraudulent OTP requests per day, providing a daily savings between $200k-$400k. We’ve thus far saved our customers close to $100M. Blocking AIT not only reduces customer expenses, it also increases conversion rates and reduces user acquisition costs.

AI Solutions Built for All Company Sizes

Whether it’s a small start up or global enterprise, anyone with an exposed API can be hit with fraud. Our products are built to detect and respond to shifts in behavior and ***begin blocking fraud within seconds*** with minimal false positives, saving a customer thousands and even millions of dollars in fraud charges.

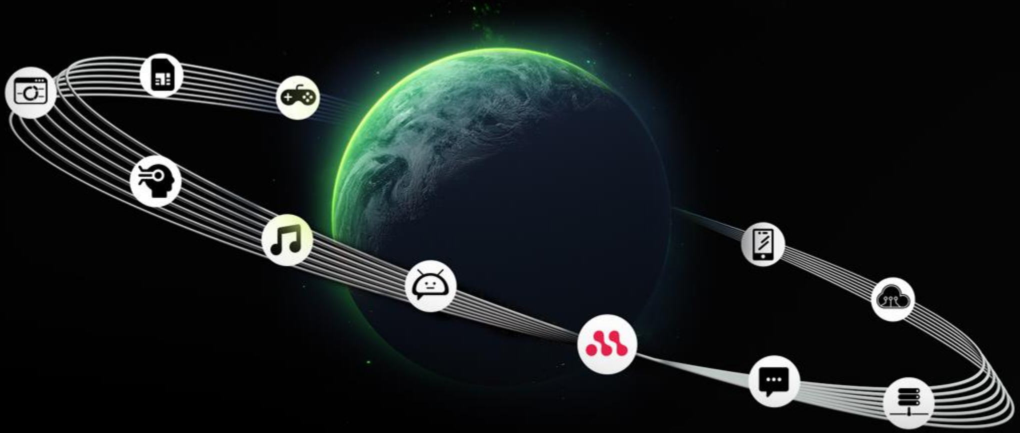
Continued Investment to Fight Against AIT

Twilio is committed to fight against AIT fraud. Some of our products come with a full guarantee against AIT fraud charges.

Monty Mobile

Imad Ismail

AIT Prevention



monty mobile
THE ART OF TELECOM

Global Connectivity Within Reach

monty mobile THE ART OF TELECOM

About Monty Mobile

A Leading Global SMS Hub, Roaming Broker and Mobile VAS Provider.

Founded in 1998 as a member of Monty Holding Group.

We work closely with worldwide mobile operators, aggregators, and enterprise to facilitate the international flow SMS across global markets.

Products & Solutions

Roaming Solutions

- Roaming Plus
- Multi-IMSI
- RID (Roaming in Dimensions)

SMS Solutions

- International A2P SMS Monetization
- A2P/P2P SMS Hub Services
- SMS Firewall
- Flash Call Blocking Solution
- Digital Verification Suite

Enterprise SMS Platform

- Monty Communication Platform
- SMS Gateway
- SMS Management Platform
- SMS Alerts

Value Added Services (VAS)

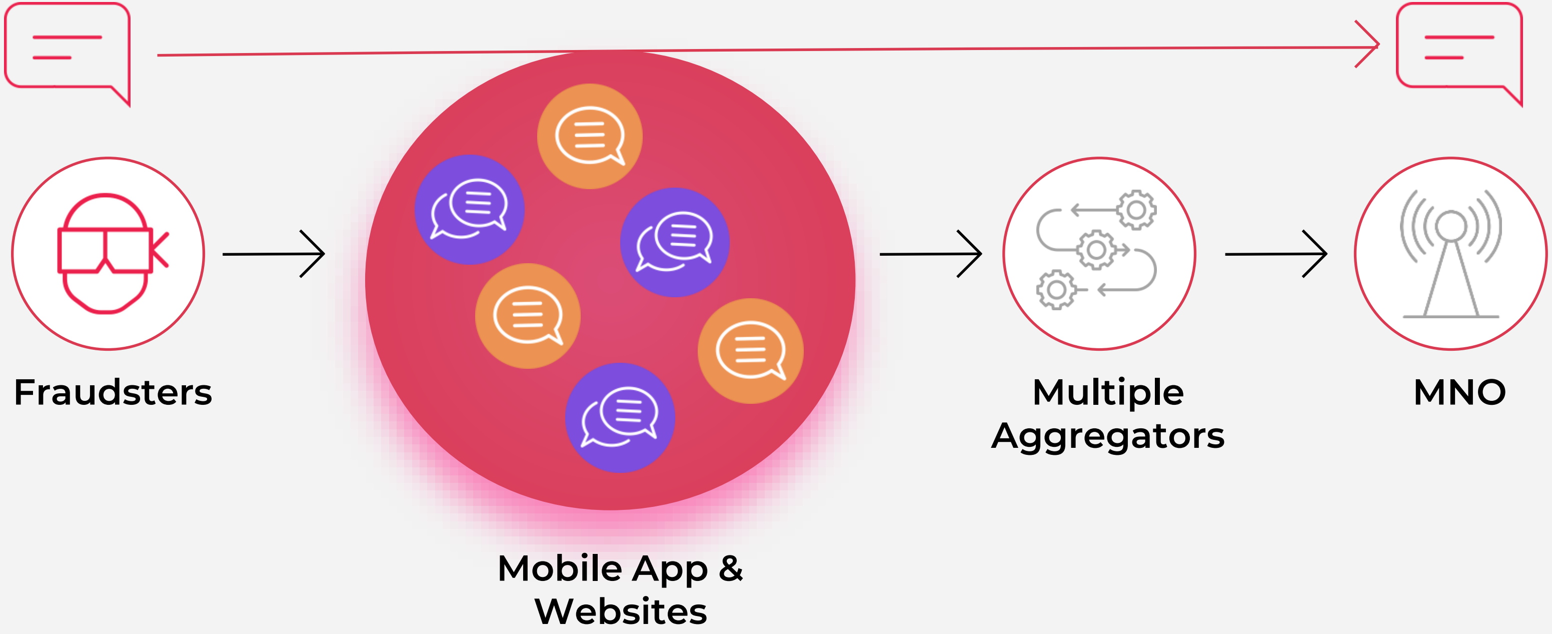
- MM Virtual Credit Card
- M-Analytics
- M-Rewards
- Revenue+
- My RBT/ M-VRBT
- Call Signature
- Self-Care App.
- Call me Back
- Back to Coverage
- Back to Coverage
- Collect Call
- Call / Data Lending
- MM Game Portal
- MVB (Mobile Virtual Banking)
- Parental Control
- Sponsored Call
- M-Challenge

Fintech

- Monty Mobile Virtual Credit Card
- Digital Wallet

eSIM Instant-Connectivity Platform

AIT Flow



Fraudsters

Mobile App & Websites

Multiple Aggregators

MNO

AIT Market Status

- Traffic Analysis
- Spikes & Anomaly Detection
- Traffic Routing Configurations

- Latest ML technologies for Auto-Detection

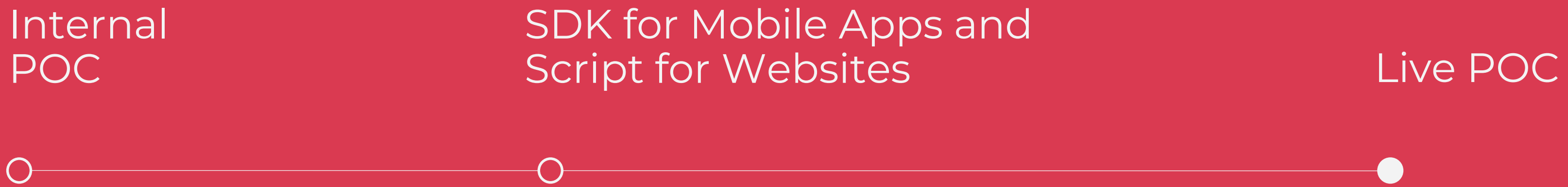
- Filtering Technologies
- Choosing Trusted Partners

- Strict Login Process (Captcha, IPs...)

AIT Detection & Prevention – App/Web Hop

- Identify the Unique Parameters/Values per each Registration
- Not to allow "Unique ID" to Register with Different Phone Numbers within X Duration
- Consider Different Bypass Mechanisms
- Business User Behavior

What’s Next?

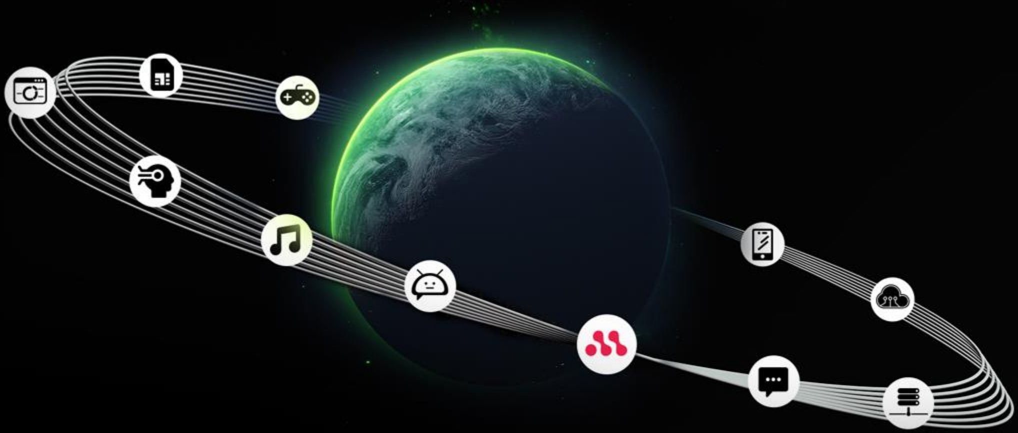


Internal POC

SDK for Mobile Apps and Script for Websites

Live POC

AIT Prevention



monty mobile
THE ART OF TELECOM

Thank You

We're here to help your business grow!

Never forget that if you have any interesting reports, press releases, updates etc. of your own, MEF can get you more brand exposure by publishing these in our regular member publications – for example, our weekly newsletter which goes out on a Friday to 15k people

Email MEF's Global Communications Manager Sam Hill – **sam@mobileecosystemforum.com**

Our Next Meeting

12th of March 2024:

Focus on potential solutions to AIT:

- **Create a compendium of commercially available anti AIT solutions for our members**
- **Identify potential AIT solutions that are currently not available in the market, which could be hosted by MEF, if necessary (non-competitive)**