AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Allegato D alla delibera n. 106/25/CONS

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui all'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Contributi pervenuti e resoconti sintetici delle riunioni

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera 457/24/CONS

Contributi al tavolo tecnico

Protocollo	Data	Partecipante	Oggetto
2025 - 0083989	01/04/2025	Omissis	Osservazioni sulla proposta di specifiche tecniche anti-spoofing del CLI (Allegato 1, Delibera 457/24/CONS)
2025 - 0089551	07/04/2025	Omissis	Nota integrativa – Riunione tecnica AGCOM del 1° aprile 2025 (Delibera n. 457/24/CONS – Proposta Omissis su blocco chiamate internazionali con CLI mobile)
2025 - 0083242	31/03/2025	Omissis	Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS – Omissis
2025 - 0085654	02/04/2025	Omissis	Consultazione pubblica di cui alla Delibera n. 457/24/CONS
E-mail	28/03/2025	Omissis	Osservazioni Omissis relative al tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS
2025 - 0082239	31/03/2025	Omissis	Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS-Osservazioni Omissis
2025 - 0081022	28/03/2025	Omissis	Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS – osservazioni di Omissis concernenti la riunione del 27 marzo 2025
E-mail	28/03/2025	Omissis	Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS

2025 - 0087118	03/04/2025	Omissis	Considerazioni Omissis a proposta di specifiche tecniche
2025 - 0091693	09/04/2025	Omissis	Consultazione pubblica di cui alla delibera n. 457/24/CONS – Osservazioni di Omissis. rispetto alle soluzioni individuate dal Tavolo Tecnico preliminare
E-mail	08/04/2025	Omissis	Delibera n. 457/24/CONS
E-mail	27/03/2025	Omissis	457/24/CONS Contributo Omissis - precedenti proposte
2025 - 0099956 2025 - 0099969	18/04/2025	Omissis / Omissis	Consultazione pubblica di cui alla delibera n. 457/24/CONS - Osservazioni rispetto alle soluzioni relative al blocco delle chiamate mobili in discussione al Tavolo Tecnico
E-mail	18/04/2025	Omissis e Omissis	Osservazioni al Tavolo tecnico AGCOM per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS
E-mail	17/04/2025	Omissis	Richiesta di informazioni relativa agli accordi CAMEL
E-mail	10/04/2025	Omissis Omissis Omissis Omissis Omissis	Osservazioni di Omissis/ Omissis - Omissis / Omissis / Omissis in merito ad alcuni elementi emersi nell'ambito dell'incontro del tavolo tecnico presso AGCOM del 15.04.2025
E-mail	17/04/2025	Omissis.	Richiesta di informazioni relativa agli accordi CAMEL
2025 - 0102404	23/04/2025	Omissis	Nota integrativa – Riunione tecnica AGCOM del prossimo 23 aprile 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

OMISSIS

Contributo al tavolo tecnico

Spett.le
Autorità per le Garanzie nelle Comunicazioni
Via Isonzo, 21/b
00198 Roma
All'attenzione del responsabile
del procedimento ***Ing. Giovanni Santella***

VIA PEC: agcom@cert.agcom.it
Omissis

Oggetto: Osservazioni sulla proposta di specifiche tecniche anti-spoofing del CLI (Allegato 1, Delibera 457/24/CONS)

Pur condividendo l'impostazione generale della proposta tecnica in relazione alla coerenza con la Delibera 457/24/CONS, **Omissis** ritiene opportuno segnalare per quanto riguarda l'efficacia delle misure tecniche di blocco previste, le seguenti considerazioni:

sebbene il tavolo tecnico attivato dall'Autorità sia limitato all'analisi delle misure di blocco previste dai commi 1 e 2 dell'art. 8, si segnala che anche il comma 4 riconosce la necessità di affrontare il tema delle chiamate con CLI nazionale **provenienti da soggetti operanti su rete IP pubblica** (ad es. servizi VoIP nomadici) reti fisse e mobili tradizionali. In questo contesto, pur in assenza di specifiche tecniche ad oggi definite, appare evidente che **l'unico approccio in grado di garantire l'affidabilità del CLI nel traffico nazionale** sia l'implementazione di un **meccanismo di autenticazione del chiamante** quali quelli basati su **STIR/SHAKEN** o protocolli equivalenti. Questa architettura — già adottata in Francia, ed in fase di valutazione in diversi paesi europei — consentirebbe di **assicurare che il numero presentato nella chiamata sia effettivamente associato all'utente mittente** e attestato da un operatore certificato. Sebbene ne siano note la complessità tecnica e la necessità di una governance centralizzata (es. autorità di certificazione), **l'inserimento di tale sistema sul traffico nazionale** costituirebbe un'evoluzione coerente rispetto alla visione "Zero Trust" già adottata per il traffico internazionale.

1. Blocco delle chiamate internazionali con CLI geografico nazionale

- **Blocco di chiamate vocali internazionali in arrivo con CLI geografico nazionale**: La proposta AGCOM prevede il **blocco sistematico** di chiamate provenienti dall'estero che mostrano un numero geografico italiano. Ciò è in piena coerenza con l'art. 8 comma 2, lett. b), che richiede di bloccare queste chiamate salvo eccezioni giustificate. Nelle specifiche si sottolinea che eventuali eccezioni

(casi leciti in cui una chiamata internazionale possa presentare un numero fisso italiano) dovranno essere **valutate e gestite con estrema cautela** caso per caso. Vi sono infatti scenari particolari – ad esempio centralini aziendali esteri che instradano chiamate mostrando il numero della sede italiana – i quali debbono però essere, a questo punto, puntualmente richiesti e **giustificati e autorizzati** esplicitamente. Omissis è favorevole alla misura di blocco delle chiamate internazionali in ingresso che presentano un **numero fisso italiano (+39 con prefisso geografico)** come CLI, la quale è ritenuta centrale per contrastare lo spoofing a danno degli utenti vittime di truffe. Queste chiamate, infatti, **non dovrebbero mai provenire dall'estero** in scenari normali: un numero di rete fissa italiana, per sua natura, genera traffico solo da linee attestatesi sul territorio nazionale. Lo **spoofing di numeri fissi** è dunque un forte indicatore di chiamata fraudolenta (ad esempio, i truffatori spesso usano numeri di call center o di enti pubblici falsificati, banche, caserme, comandi di polizia, etc). La proposta tecnica rende **mandatorio** il blocco di tali chiamate, salvo eccezioni documentate. Questo approccio è pienamente condivisibile: impedisce al chiamante malevolo di far apparire numeri di telefono locali (città, banche, uffici) come esca, proteggendo l'utente dal cadere in inganno. **Una raccomandazione migliorativa** potrebbe essere di *predisporre un chiaro framework per le eccezioni*: ad esempio, definire procedure affinché un operatore o un soggetto richieda l'autorizzazione per inviare traffico con CLI fisso italiano dall'estero (documentando il motivo lecito). Queste richieste - come si diceva - dovrebbero essere soggette ad approvazione e potrebbero essere gestite con un meccanismo inter-operatore simile alla MNP oltre segnalate all'Autorità per opportuno monitoraggio, i numeri autorizzati potrebbero essere gestiti in whitelist condivise. Fuori da tali eccezioni, il default rimarrebbe il blocco e, in caso di irregolarità emerse nel monitoraggio, il numero autorizzato dovrebbe essere prontamente espunto dalla whitelist. Si suggerisce altresì di chiarire le modalità di gestione delle eccezioni: se tramite blocco con eccezioni manuali preferita dalla scrivente, o tramite anonimizzazione automatica in casi dubbi.

2. Blocco delle chiamate internazionali con CLI mobile nazionale

- **Blocco di chiamate vocali internazionali in arrivo con CLI mobile nazionale (+393…)**: È la parte più delicata, poiché l'art. 8 comma 2, lett. c) consente il blocco solo dopo verifica che l'utente non sia realmente all'estero in roaming. La proposta tecnica risponde a questo requisito introducendo un meccanismo di **query in tempo reale tra operatori** per controllare lo stato dell'utenza mobile associata al CLI chiamante. In pratica, il carrier internazionale che introduce la chiamata in Italia interroga la rete dell'operatore mobile titolare di quel numero per determinare se la chiamata sia possibile o meno (ad es. verificando se l'utenza è in roaming, attiva, registrata, ecc.) Se la verifica conferma che il numero **non dovrebbe originare chiamate dall'estero** (perché, ad esempio, l'utente è

registrato sul territorio nazionale, o il numero non è attivo/in uso), allora la chiamata viene bloccata. Riteniamo questo approccio di **autenticazione del CLI tramite query** del tutto coerente con la previsione normativa di controllare il roaming nel rispetto della privacy e bloccare le chiamate con CLI mobile falsificato. La proposta dettaglia vari casi: ad esempio, blocco immediato se il numero non risulta attivo o assegnato in quel momento (numero non in uso), oppure se l'utente risulta connesso in Italia (non in roaming). Sono previsti inoltre controlli sullo **stato di registrazione** dell'utenza: se il cliente mobile risulta offline (nessuna registrazione né in Italia né su rete estera 2G/3G, segno che ha il telefono spento), qualsiasi chiamata internazionale col suo CLI viene bloccata poiché l'utente non potrebbe generare. Queste condizioni implementano dunque fedelmente l'art. 8 e sembrano garantire che vengano bloccate le chiamate presumibilmente spoofing senza impattare le chiamate lecite di utenti realmente in roaming. È importante notare che la norma richiede di salvaguardare le chiamate legittime: la proposta infatti specifica che le misure non devono compromettere il corretto instradamento delle chiamate internazionali lecite né bloccare eccezioni consentite. Il sistema di query serve proprio a distinguere con buona approssimazione le chiamate reali da quelle falsificate, riducendo al minimo i falsi positivi. Per le chiamate con **CLI mobile italiano (+39 3XX)** provenienti dall'estero, la soluzione proposta adotta un meccanismo dinamico di verifica, riconosciuto anche a livello internazionale come il più efficace per distinguere le chiamate spoofing da quelle genuine in presenza di utenti roaming. A differenza dei numeri fissi, infatti, un numero mobile italiano *può* legittimamente originare una chiamata dall'estero (quando l'utente è in roaming internazionale). Pertanto, la misura non può essere un blocco incondizionato: occorre discriminare caso per caso in **tempo reale** lo **stato dell'utenza mobile**.

- **Meccanismo della *query* tra operatori:** Il sistema architettato prevede che gli **operatori di transito internazionale autorizzati** (cioè, i carrier che ricevono chiamate dall'estero per terminazione in Italia) effettuino una *query* verso l'operatore mobile italiano detentore del numero presentato come CLI. In pratica: se arriva una chiamata internazionale con CLI +39 3… (mobile), il carrier di ingresso identifica quale operatore nazionale gestisce quella numerazione (tenendo conto dell'eventuale **portabilità del numero** in base al database OLO nazionale) e interroga un'apposita API esposta da tale operatore per chiedere se la chiamata debba essere bloccata oppure no. L'operatore mobile verifica nei propri sistemi lo stato dell'utenza chiamante e restituisce un responso **"BLOCCO" o "NO BLOCCO"** entro pochi millisecondi. In base alla risposta, il carrier deciderà se instradare la chiamata al destinatario in Italia oppure interromperla. Questo tipo di architettura (spesso chiamata **"Screening in real-time"** del CLI), dove il

database di portabilità è utilizzato per costruire un proxy che interroga lo stato delle utenze mobili prima di far passare le chiamate.

- **Casi di blocco e logica decisionale:** la documentazione tecnica dettaglia le condizioni in base alle quali la risposta alla query sarà di blocco della chiamata, riflettendo le casistiche previste dalla norma e le esperienze pratiche:

  - ✓ **Numero non valido o non attivo**: se il numero mobile indicato come chiamante **non risulta attivo** sulla rete dell'operatore proprietario (es. numero inesistente, disattivato, non più assegnato a un cliente) la chiamata deve essere bloccata.

  - ✓ **Utenza registrata in Italia (non in roaming)**: se il cliente mobile proprietario del numero CLI è connesso sulla rete domestica (registrato su celle in Italia), significa che non sta effettuando la chiamata dall'estero. In tal caso, qualsiasi chiamata che arrivi da un gateway internazionale con quel CLI è illegittima e va **bloccata**. Questa regola attua fedelmente l'art. 8. comma 2: l'autorità richiede il blocco dopo aver verificato che l'utente finale non sia in roaming all'estero.

  - ✓ **Utenza non registrata affatto (telefono spento/non raggiungibile)**: se l'utente mobile in questione **non risulta registrato su alcuna rete** in quel momento (né in patria né in roaming), ciò implica che ha il telefono spento o comunque non è agganciato alla rete; dunque, non potrebbe in nessun caso aver originato una chiamata. La proposta indica di verificare in particolare l'assenza di registrazione su rete 2G/3G, poiché in architettura di rete mobile tradizionale è tramite queste tecnologie (circuit-switch) che una chiamata vocale verrebbe veicolata su interconnessione internazionale. In altri termini, se l'utente non ha alcuna sessione CS attiva (ad esempio perché completamente offline), una chiamata internazionale col suo numero è necessariamente uno spoofing e va bloccata. Questa regola copre scenari come l'utente che ha la SIM spenta o fuori copertura: situazione che i truffatori potrebbero sfruttare il blocco di chiamate col CLI di utenti offline è quindi cruciale per colmare quel varco.

  - ✓ **Ulteriori controlli facoltativi (roaming 4G)**: la proposta include anche un controllo aggiuntivo, indicato come **non mandatorio**, relativo agli utenti registrati all'estero esclusivamente su rete 4G/VoLTE. Questo nasce dal fatto che, con l'evoluzione tecnologica, molti operatori gestiscono il roaming voce tramite **VoLTE con architettura S8HR (S8 Home Routing)**: in tale modello, le chiamate dei clienti in roaming non vengono instradate

tramite gateway circuitali internazionali, ma viaggiano come traffico dati fino al paese di origine, dove l'operatore home le tratta come chiamate nazionali. Ciò implica che **un utente in roaming 4G puro non genererà mai una chiamata che appaia come proveniente da un trunk internazionale tradizionale**, bensì la sua chiamata giungerà direttamente dalla rete domestica (anche se l'utente si trova fisicamente all'estero). Dunque, se arriva sul gateway internazionale italiano una chiamata con CLI mobile X e l'operatore vede che l'utente X è registrato all'estero ma solo su IMS/4G (senza fallback 2G/3G), con alta probabilità quella chiamata è spoofing. La misura opzionale suggerisce di bloccare anche queste chiamate "impossibili", l'azione è lasciata alla discrezionalità dell'operatore ("best effort"), **una raccomandazione migliorativa** potrebbe essere di rendere anche questo controllo **mandatorio** per l'operatore mobile. Se l'operatore sa, ad esempio, che l'utente è in un paese dove non esistono reti 2G/3G (dunque se è registrato, lo è solo in 4G), può scegliere di bloccare eventuali chiamate col suo CLI provenienti da percorsi TDM tradizionali.

Importante, secondo la scrivente, chiarire quali siano gli obblighi dell'operatore negli scenari previsti dalla slide 9 punto 2), si nota che l'operatore ha la "facoltà" di rispondere con il blocco della chiamata. La formulazione testuale sembrerebbe prevedere che l'operatore possa anche non rispondere in caso non intenda bloccare la chiamata. Se fosse così si rischierebbe di legittimare uno scenario in cui l'operatore, potendo non rispondere, non effettua i controlli previsti. Si suggerisce allora di chiarire che, l'operatore ha comunque l'obbligo **di rispondere alla query.** Non si comprende inoltre il punto a) n. 3) della medesima slide 9: nel punto 2) si prevede che l'operatore risponda con l'ordine di "BLOCCO DELLA CHIAMATA" e si prevedono le relative eccezioni. Al punto 3) si prevede il "NON BLOCCO "in casi **diversi dai precedenti**" (precedenti potrebbe essere riferito ai punti 2) comprendendo anche gli scenari indicati nel sotto elenco i), ii) e iii). **occorre invece chiarire che il punto 3) si riferisce esclusivamente ai casi previsti al punto 1) e alla prima parte del punto 2).**

Nel complesso, la logica di decisione implementata attraverso le query appare **solida e calibrata**: copre i casi più evidenti di spoofing (numero inesistente, utente in Italia, utente offline) come obbligatori, e considera come ulteriore difesa quelli più avanzati (utente in roaming IMS) su base opzionale, a nostro avviso da rendere mandatori.

È importante ricordare che negli ultimi anni diversi paesi hanno adottato un approccio "zero trust" per contrastare le chiamate fraudolente **spoofing**. Questo approccio prevede che l'**operatore ricevente** (cioè, l'operatore di destinazione nel paese chiamato) blocchi direttamente questo tipo di chiamate *in ingresso*, senza passare dal Carrier Internazionale Autorizzato.

Di seguito esaminiamo vantaggi e limiti di tale approccio:

- **Semplicità e autonomia operativa**: Far gestire il blocco all'operatore ricevente significa che **ciascun operatore può agire in autonomia** per proteggere i propri utenti, senza dover attendere che tutti gli altri (originating carrier, carrier di transito, ecc.) implementino qualcosa. Tecnicamente, implementare una regola di blocco/sostituzione CLI sui propri switch o SBC è relativamente semplice: molti operatori hanno già "liste nere" di numerazioni anomale o controlli di formato che possono estendere a questo caso. Ciò evita di dover instaurare complesse query in tempo reale tra operatori per validare ogni chiamata, ma solo le chiamate proveniente da altri operatori, ad esempio, un operatore mobile può incrociare il filtro con i dati del proprio HLR per *consentire* le chiamate dei propri clienti in roaming (sapendo in tempo reale chi dei suoi numeri mobili si trova all'estero). In altre parole, **l'interoperabilità viene ottenuta "per sottrazione"**, filtrando ciò che non è conforme a regole condivise (es. *un numero nazionale non deve entrare da interconnessioni internazionali.* Questo approccio riduce la dipendenza da infrastrutture centralizzate accelerando i tempi di implementazione.
- **Impatto su ricavi degli operatori e sul traffico**: Bloccare più chiamate significa in teoria **meno traffico terminato e quindi meno ricavi da terminazione** per gli operatori. Alcuni provider potrebbero essere riluttanti ad auto-imporsi filtri che tagliano minuti (soprattutto quei **carrier internazionali** che guadagnano proprio dall'instradare volumi, talvolta anche di qualità dubbia). Laddove un operatore consegni una chiamata con CLI falso, si dovrebbe prevedere contrattualmente l'obbligo di storno degli importi per la terminazione della chiamata in questione, anche a posteriori.

3. Gestione dell'impatto operativo sulle reti mobili

L'introduzione dei meccanismi proposti ha delle implicazioni operative importanti per le reti sia mobili che di transito:

- **Prestazioni e tempi di risposta**: Un punto critico è garantire che la query non introduca un ritardo significativo nel *setup* della chiamata. La consultazione al volo dell'operatore mobile aggiunge un passaggio in più nel signaling: idealmente il tutto deve avvenire nell'ordine di qualche decina di millisecondi. La proposta cita espressamente la necessità di definire l'**allungamento "sostenibile" del tempo di stabilimento chiamata** dovuto a questa procedura. In pratica, occorre dimensionare i sistemi in modo che la risposta all'API arrivi velocemente (es. <100 ms).

Fortunatamente, le odierne reti mobili dispongono già di funzionalità di interrogazione veloce (si pensi alle *HLR Lookup* usate per gli SMS Home Routing): queste potrebbero essere riutilizzate o adattate. Per assicurare le performance, È opportuno anche stabilire cosa succede se la query non riceve risposta entro il timeout (ad es. per problemi di rete): in genere, per non rischiare di bloccare chiamate legittime, si potrebbe impostare una **politica di fail-safe** (ossia, in caso di mancata risposta dall'API, la chiamata viene comunque instradata). Questa scelta però comporta un rischio di sicurezza (un malintenzionato potrebbe tentare di bypassare il controllo causando il fallimento). Una soluzione bilanciata potrebbe essere: tempi di timeout molto stringenti e *ridondanza* delle query (più tentativi magari su endpoint diversi), e nel medio termine l'analisi statistica di eventuali pattern di "mancata risposta" sospetti.

- **Carico di segnalazione**: Le reti dovranno gestire un incremento di messaggi di segnalazione. Ogni chiamata internazionale con CLI +39 mobile genera una query verso l'operatore mobile: se pensiamo a volumi nell'ordine di milioni di chiamate al giorno a livello di sistema paese, anche le query saranno dell'ordine di milioni. Gli operatori dovranno dimensionare server e database per rispondere a picchi di traffico di interrogazioni. È importante che ogni operatore **monitori accuratamente** l'utilizzo dell'API, per eventualmente tarare capacità extra o mitigare abusi. A tal fine, potrà essere utile inserire nell'API meccanismi di controllo accessi e *rate limiting* per ciascun carrier internazionale, prevenendo tempeste di query fuori dal normale scenario di chiamate.
- **Necessità di adesione universale**: Un punto critico, già sollevato anche nel documento Allegato 1, è che queste misure funzionano solo se **tutti gli operatori coinvolti le adottano**. Sembrerebbe improprio, al punto 4) della slide 9, prevedere che il Carrier Internazionale Autorizzato possa far passare la chiamata se l'operatore mobile non risponde: ciò rischia di consentire agli operatori mobili di non evadere le query. Si propone sia previsto sempre l'obbligo di risposta alla query con BLOCCO/NON BLOCCO. Basta un varco lasciato aperto da un operatore per vanificare parte della protezione: se un carrier internazionale in Italia non implementasse il blocco, i truffatori veicolerebbero il traffico attraverso di esso; se un operatore mobile non fornisse risposte affidabili, i controlli sui suoi numeri sarebbero aggirabili. Per questo la delibera e l'Allegato 1 insistono sulla cooperazione e sulla standardizzazione della soluzione. La **sostenibilità tecnica** di questa soluzione dipende quindi sia dalla robustezza intrinseca (prestazioni, accuratezza) sia dal coordinamento multi-operatore.

In sintesi, la soluzione basata su query in tempo reale appare **fattibile e ben ponderata**. Essa

garantisce un elevato tasso di intercettazione dello spoofing sui mobili, mantenendo la continuità di servizio per gli utenti in roaming reale. L'esperienza di altri paesi che l'hanno adottata (o la stanno adottando) conferma che è una strada praticabile ed efficace. Sarà importante, in fase di attuazione, condurre test con traffico reale e affinarne i parametri per massimizzare il rapporto tra **blocchi fraudolenti** e **chiamate legittime lasciate passare**.

4. Privacy, sicurezza dei dati e tutela dell'utente

L'implementazione di misure anti-spoofing deve necessariamente tenere conto delle **implicazioni di privacy** e tutela dei dati personali, poiché coinvolge informazioni sullo stato delle utenze (ad esempio se un dato numero è attivo, in Italia o all'estero). La normativa vigente (GDPR, direttiva ePrivacy) impone che il trattamento di dati relativi a localizzazione e stato dell'utente avvenga con una base giuridica solida e minimizzando i dati trattati. In questo contesto, la Delibera AGCOM costituisce già una base legale specifica che **autorizza gli operatori** a svolgere tali controlli per motivi di sicurezza e tutela utenti. L'art. 8 comma 2(c) esplicitamente vincola i controlli sullo stato di roaming al **rispetto delle disposizioni sulla privacy pertinenti**, evidenziando la consapevolezza del tema.

La proposta tecnica adotta alcuni accorgimenti fondamentali per garantire la conformità privacy:

- **Risposta binaria SI/NO (block or allow)**: L'API di verifica non fornisce dati personali dettagliati (es. posizione esatta dell'utente o il suo operatore estero), ma semplicemente un'indicazione di blocco sì/no sulla chiamata. Ciò è conforme al principio di **minimizzazione**: l'operatore di transito che interroga non viene a conoscenza di alcuna informazione aggiuntiva sull'utente, se non il fatto che la chiamata può o non può passare. In altre parole, l'architettura può essere realizzata in forma di **query a conoscenza zero**: a ogni interrogazione corrisponde solo un esito utile a instradare la chiamata, senza rivelare il perché (es. "utente non in roaming" oppure "numero inesistente") né altri dettagli sensibili.
- **Niente archivi centralizzati di utenti in roaming**: Piuttosto che mantenere un database centralizzato degli utenti italiani attualmente all'estero (che potrebbe destare preoccupazioni dal punto di vista concorrenziale e privacy), si è scelto un meccanismo *on demand*. Ogni verifica è istantanea sul singolo numero, e gestita dal legittimo custode di quell'informazione (l'operatore mobile stesso). Questo impedisce che un operatore possa costruire un elenco dei clienti di altri operatori e dei loro stati. Idealmente – ed è una proposta sostenuta da Omissis – il sistema potrebbe essere gestito da un ente terzo indipendente (sul modello del Registro delle Opposizioni gestito dalla Fondazione Ugo Bordoni) che faccia da **proxy neutrale** per tutte le query.

In tal modo si centralizzerebbe il servizio senza concentrare i dati sensibili presso un concorrente. Il proxy stesso opererebbe in modalità "zero- knowledge", come descritto, rendendo impossibile risalire a dati di dettaglio anche per chi lo gestisce. Questa soluzione apporterebbe un ulteriore livello di fiducia e tutela della riservatezza. Nell'Allegato 1 attuale, tuttavia, sembra prevalere un modello di interrogazioni bilaterali dirette tra carrier e operatori mobili, con obbligo per i carrier di dichiarare e notificare tale attività. Anche questo modello è lecito, purché – come detto – vincolato a stretti requisiti di sicurezza e trasparenza.

- **Sicurezza delle interfacce e prevenzione abusi**: Trattandosi di un'API inter-operatori, sarà importante implementare misure di sicurezza informatica robuste. Ogni chiamata di verifica deve essere **autenticata e autorizzata**: solo i soggetti autorizzati (carrier internazionali registrati) potranno effettuare query, magari tramite certificati digitali o VPN dedicate. Inoltre, andranno loggate le richieste in modo sicuro, per poter rilevare eventuali usi impropri (ad esempio interrogazioni massive di numeri senza chiamate corrispondenti, che potrebbero indicare tentativi di profiling). Idealmente, la query dovrebbe contenere anche informazioni contestuali alla chiamata (ad es. identificativo di chiamata o tronco d'ingresso) per evitare che qualcuno possa simulare una query al di fuori di un reale evento di chiamata. Questi dettagli implementativi dovranno emergere nelle specifiche definitive.
- **Informativa all'utente e principi di proporzionalità**: Dal punto di vista dell'utente finale, queste misure sono **trasparenti** e non richiedono un suo intervento, ma coinvolgono i suoi dati in modo indiretto. Sarebbe buona norma che gli operatori integrino nelle proprie informative privacy una menzione di questi trattamenti finalizzati alla sicurezza (*fraud prevention*), indicando che il numero di telefono potrebbe essere oggetto di verifiche di autenticità quando usato come identificativo di chiamata, a tutela dell'utente stesso. In termini di proporzionalità, il beneficio (riduzione drastica delle truffe **vishing** e telemarketing ingannevole) supera l'intrusività molto limitata del controllo (che, come detto, **non rivela informazioni personali all'esterno** e non incide su comunicazioni lecite).

In aggiunta, va considerato l'effetto di queste misure sulla **privacy "percepita" dall'utente**: ad esempio, un utente in roaming che fosse soggetto a blocco ingiustificato potrebbe percepire una limitazione. È quindi essenziale che i falsi positivi siano minimizzati e possibilmente **tracciati**. Un suggerimento potrebbe essere quello di prevedere, per le chiamate bloccate, la disponibilità di un log interno che permetta agli operatori di individuare se qualche chiamata legittima è stata erroneamente filtrata (es. un cliente segnala che dall'estero non riusciva a chiamare con il proprio numero: l'operatore mobile, verificando i log, potrebbe capire se la chiamata è stata marcata erroneamente come spoofing e correggere eventuali regole).

Ovviamente tali log devono essere accessibili solo per fini di verifica tecnica e non per altri scopi.

In conclusione, su questo punto, la proposta appare **consapevole dei vincoli privacy** e costruita per rispettarli (minimizzazione del dato, finalità specifica di sicurezza, controlli accessi). Con l'adozione di un possibile **ente terzo di gestione** e delle opportune misure di sicurezza informatica, le soluzioni anti-spoofing potranno operare garantendo sia la protezione dell'utenza dalle frodi sia la tutela dei dati personali secondo la normativa vigente.

5. Criticità dal punto di vista normativo e attuazione delle soluzioni per fasi

- **Necessità di chiarezza circa i soggetti che sarebbero sanzionati e circa la natura della violazione**: Il sistema proposto fa affidamento sulle attività di quelli che sono definiti "Carrier Internazionali Autorizzati in Italia" (che in alcuni casi coincidono con gli operatori nazionali che forniscono il servizio all'utente finale, in altri no). La definizione di "Carrier Internazionali Autorizzati in Italia" è diversa dalla definizione di "operatore" contenuta nella bozza di Regolamento e ciò potrebbe portare a paradossi e discrasie interpretative. Si propone di chiarire che le sanzioni di cui all'art. 9 si applicano sia agli Operatori Internazionali, sia gli operatori fissi, che agli operatori mobili. In base alla definizione di cui all'art. 1 f) dell'Allegato B alla Delibera 457/24, sembrerebbe, infatti, che le sanzioni siano applicabili esclusivamente agli "operatori che forniscono agli utenti finali servizi di comunicazione elettronica", con il risultato che alcuni Operatori Internazionali non potrebbero essere sanzionati per la violazione. Inoltre, nel caso di operatori esteri che operano e sono autorizzati in Italia attraverso filiali locali, il riferimento di cui all'art. 30 comma 19 del CCE alla sanzione parametrata al fatturato "della società" potrebbe puntare ad un fatturato minimo nei casi in cui i ricavi dell'attività di operatore internazionale siano imputati a diversa società da quella autorizzata in Italia e così minare l'efficacia dell'enforcement e la deterrenza del provvedimento anti- spoofing. Si propone di chiarire che le sanzioni verranno parametrate sul fatturato globale della società riferibile all'Operatore Internazionale, che abbia effettivamente fatturato l'attività di transito verso Italia delle chiamate. Si potrebbe anche configurare la violazione come responsabilità in solido tra tutti gli operatori nazionali che abbiano concorso ai controlli previsti dalla procedura;

- **Il Regolamento di cui all'Allegato B della Delibera 457/24 prevede all'art. 8 esclusivamente obblighi di "adottare" le misure di blocco**: non è chiaro dal testo se per "adozione" si intenda anche effettivo e puntuale utilizzo delle procedure adottate In sostanza, la bozza di Regolamento non sembra prevedere sanzioni specifiche in caso, pur avendo adottato formalmente le procedure, le chiamate con CLI

falso continuino a passare e nemmeno specifiche sanzioni per il mancato blocco di CLI che avrebbero dovuto essere bloccati. Si propone di chiarire che la sanzione è applicabile non soltanto se non siano adottate le misure di blocco, ma anche se le procedure previste da AGCOM non siano correttamente eseguite, con il risultato di chiamate massive con CLI falso che riescono ad essere terminate e/o mancata risposta alle query che arrivano all'operatore mobile.

- **L'attuazione delle soluzioni per fasi:** si esprime perplessità circa la decisione di attuare le soluzioni a fasi (**"Blocchi con CLI non mobili che non richiedono query tra operatori"** e **"Blocchi con CLI mobili che richiedono query con operatori"**, ripartito quest'ultimo in fase 1 (query di blocco per chiamate con numeri NON assegnati da MIMIT) e fase 2 (query di blocco per chiamate con numeri assegnati ad un operatore mobile), e di "spacchettare" quindi la discussione sulle procedure per la conformità all'art. 8 comma 2 del proposto Regolamento allegato alla Delibera 457/24 dalla discussione per la conformità all'art. 8 comma 4 del medesimo proposto Regolamento. Non va, sottovalutato il rischio concreto che l'implementazione dei blocchi dei CLI mobili appartenenti ad archi di numerazioni non assegnati da MIMIT ad alcun operatore mobile e non a standard ITU e geografici/non geografici diversi da mobili, porti gli spoofers a variare le proprie modalità di comportamento concentrarsi sull'adottare archi di numerazioni assegnate ad operatore mobile e attivi, in assenza di specifici controlli a riguardo nell'attesa della fase 2, falsificando numeri di utenti reali, le malcapitate vittime sarebbero costretti a provare di non essere stati loro gli autori delle chiamate, con estremo disagio, ampliando le platea delle vittime che oltre il cittadino disturbato e/o truffato di queste pratiche odiose, si aggiunge anche l'ignaro e legittimo titolare dell'utenza mobile attiva. Al riguardo, la scrivente, formula le seguenti proposte:

  - ✓ Si potrebbe, a stretto giro, implementare solo il blocco dei CLI diversi dai numeri mobili ed entranti dall'estero e, successivamente, una volta definito il complesso delle misure che riguarda il blocco dei CLI mobili - sia quelli entranti da rete estera, sia quelli originati all'interno del territorio, implementare il blocco dei CLI mobili. La proposta ripartizione risulterebbe, ad avviso di Omissis-, meglio comprensibile all'utenza - la quale potrebbe essere avvisata che la chiamata da "fisso" è diventata sicura ed affidabile e nel seguito diventerà sicura ed affidabile anche la chiamata proveniente da CLI mobile.

  - ✓ Avviare le misure assieme, a meno che le tempistiche di definizione ed implementazione della soluzione completa, rendano ragionevole e possibili.

In sostanza, mettere in sicurezza solo una parte delle chiamate da CLI mobile assieme ai fissi, non avrebbe senso, poiché non si potrebbe garantire nulla circa l'affidabilità del CLI mobile all'utente destinatario della chiamata e dunque, il pubblico faticherebbe a comprendere l'utilità di tale "blocco" finché esso rimane largamente permeabile; ciò probabilmente sarebbe, anzi, motivo di critica verso gli operatori e le imprese della filiera del telemarketing, per l'errata impressione che non sia stato raggiunto l'obiettivo. Anche per tale motivo, qualsiasi la suddivisione delle fasi del blocco che si decida di adottare, essa dovrebbe essere accompagnata da procedure antifrode per traffico estero anomalo su CLI di utenze attive, seguite dagli operatori mobili a tutela della propria clientela. Poiché, nonostante l'imponente sistema ipotizzato, residuano ipotesi di spoofing con **numeri mobili esistenti** sfruttando eventuali vulnerabilità dei sistemi di piccoli operatori, si propone di istituire un sistema di segnalazione dello spoofing sul modello del "piracy shield" di AGCOM per segnalazioni veloci a disposizione dell'utenza, ad esempio una piattaforma sotto l'egida di AGCOM, dei CLI manipolati i cui risultati - quando statisticamente significativi - es. plurime segnalazioni del medesimo CLI nella medesima giornata - portino a specifici controlli su quale sia l'operatore che ha consegnato la chiamata con CLI camuffato massivamente, a cui AGCOM potrebbe così compiere gli opportuni accertamenti. Allo stesso modo sarebbe necessaria una particolare tutela per numerazioni **mobile** e **geografiche sensibili** di enti pubblici, persone che ricoprono incarichi istituzionali, istituti bancari, ecc. con sanzioni rafforzate.

6. Ulteriori proposte rafforzative del sistema

La bozza di specifiche tecniche analizzata appare nel complesso coerente con le esigenze normative. Le potenziali criticità (attuazione delle soluzioni per fasi, interoperabilità a livello di operatore ricevente, latenza delle API, gestione del roaming su rete 4G/VoLTE mandatorio, coordinamento multiparte) sono note e affrontabili con la collaborazione di tutti i soggetti interessati. Implementando i suggerimenti sopra esposti – in particolare superare la **criticità rilevante** dell'attuazione delle soluzioni per fasi – l'Italia può dotarsi di un sistema efficace per **arginare il fenomeno dello spoofing del chiamante**, proteggendo sia i consumatori da truffe e telemarketing abusivo, sia la fiducia complessiva nel servizio telefonico. Le misure proposte miglioreranno la **trasparenza dell'identificazione del chiamante**, obiettivo ultimo dell'art. 8, ripristinando la **corretta corrispondenza tra numero visualizzato e chiamante reale** e riducendo l'anonimato fraudolento che finora ha alimentato abusi impuniti. Con queste premesse, il quadro italiano anti-spoofing potrà divenire un **modello di riferimento** anche oltre confine per contrastare le chiamate falsificate e riconquistare la fiducia degli utenti nelle comunicazioni telefoniche. Di seguito si riepilogano alcuni **suggerimenti migliorativi e alternative praticabili** emersi dall'analisi, che potrebbero essere considerati per ottimizzare ulteriormente l'efficacia e la sostenibilità delle misure:

- **Soluzione centralizzata tramite ente terzo (proxy)**: la creazione di un **hub centralizzato indipendente** per le interrogazioni relative alle query (con CLI non

mobili), che potrebbe semplificare l'implementazione e aumentare la fiducia reciproca tra operatori. Un ente terzo (un soggetto neutrale designato da AGCOM) potrebbe gestire un servizio in cui: il carrier internazionale invia la query all'hub, l'hub individua l'operatore mobile competente (grazie ai dati di portabilità) e inoltra la richiesta, raccoglie la risposta e la ritrasmette al richiedente. Questo modello "proxy" ha il vantaggio verificare tutte le chiamate proveniente dall'estero indipendente dalla volontà del Carrier Internazionale, di ridurre il numero di interfacce (ogni carrier si integra una volta con il proxy, invece di stipulare connessioni con 4-5 diversi operatori mobili) e di occultare agli operatori mobili l'identità commerciale di chi origina la query e viceversa (ulteriore garanzia di riservatezza).

- **Gestire l'interoperabilità a livello di operatore ricevente per query (con CLI mobile)**: i vantaggi includono una protezione più immediata per gli utenti e meno dipendenza da soluzioni complesse inter-operatori.
- **Coinvolgimento della comunità scientifica/tecnologica**: sarebbero auspicabile utilizzi di **intelligenza artificiale e machine learning** per riconoscere schemi di chiamate anomali, che si potrebbe sin d'ora prevedere un monitoraggio statistico degli eventi di spoofing rilevati. Gli operatori, ad esempio, potrebbero condividere in forma aggregata dati sul numero di chiamate bloccate, sulla distribuzione geografica delle origini sospette, sugli orari di picco, ecc. Queste informazioni potrebbero alimentare studi e modelli predittivi per anticipare nuove forme di attacco. Un'idea pratica potrebbe essere l'istituzione di un **Osservatorio sullo spoofing** sotto l'egida di AGCOM, che raccolga periodicamente tali dati e coinvolga esperti per analizzarli. Ciò manterrebbe l'Italia all'avanguardia anche nell'evoluzione successiva delle contromisure.

- **Chiarezza verso gli utenti finali**: Pur trattandosi di misure di rete, senza impatto diretto sull'uso da parte dell'utente, un'azione di comunicazione potrebbe aumentare la fiducia del pubblico. Informare gli utenti che è in atto un sistema di controllo anti-spoofing (magari tramite comunicati stampa o tramite i canali informativi degli operatori) può sia rassicurare – mostrando l'impegno nel proteggerli – sia educare: ad esempio spiegando che, dopo l'introduzione di queste misure, *qualora ricevessero ancora chiamate con numeri italiani sospetti dall'estero, probabilmente si tratta di tentativi molto sofisticati*. In altre parole, la trasparenza sulle azioni intraprese può essere parte della tutela del consumatore. Al contempo, gli utenti vanno incoraggiati a continuare a segnalare eventuali chiamate moleste o sospette, perché il loro feed back sarà utile per affinare i filtri.

7. Conclusione

Omissis- raccomanda pertanto che:

1. Si coordini il testo del Regolamento Allegato B alla Delibera 457/24 con quanto previsto dalla procedura, specie per la parte relativa alle definizioni e alle sanzioni e si chiariscano nel dettaglio quali sono i comportamenti oggetto di sanzione e quali gli operatori interessati (nazionali/internazionali).
2. Si preveda un diverso timing di attuazione delle soluzioni per fasi
3. Si valuti di prevedere l'obbligo di risposta a ogni query a carico degli operatori nazionali in maniera da non ingenerare situazioni di incertezza interpretativa ed operativa.
4. Sia avviato un tavolo tecnico permanente tra operatori mobili per definire regole comuni di validazione e blocco anche per le chiamate IP/IMS.
5. Sia istituito un sistema di segnalazione "veloce" disponibile all'utenza nei termini descritti nel presente documento;

Con l'occasione, ringraziandoVi per l'attenzione dedicata e confidando che questi chiarimenti possano risultare utili ai fini dell'analisi in corso, si resta a disposizione per qualsiasi ulteriore informazione o approfondimento ritenuto necessario.

Roma 31 marzo 2025

OMISSIS Distinti saluti,

OMISSIS

Spett.le
Autorità per le Garanzie nelle Comunicazioni
Via Isonzo, 21/b
00198 Roma
All'attenzione del responsabile
del procedimento ***Ing. Giovanni Santella***

VIA PEC: agcom@cert.agcom.it
Omissis

Oggetto: Nota integrativa – Riunione tecnica AGCOM del 1° aprile 2025 (Delibera n. 457/24/CONS – Proposta OMISSIS su blocco chiamate internazionali con CLI mobile)

La scrivente **Associazione Omissis-** fa riferimento alla partecipazione alla riunione tecnica indetta da codesta Autorità in data 1° aprile 2025, avente ad oggetto la proposta presentata da OMISSIS basata sul "modello belga" per il blocco delle chiamate internazionali recanti un CLI mobile italiano. Con la presente, si intendono ribadire in forma scritta le posizioni di Omissis già espresse in tale sede e fornire ulteriori elementi di valutazione in merito.

1. Partecipazione alla riunione tecnica del 1° aprile 2025

L'incontro ha esaminato la proposta avanzata da Omissis., ispirata all'esperienza belga, concernente il blocco sistematico delle chiamate **internazionali in ingresso con CLI mobile nazionale**. Omissis ha attivamente contribuito alla discussione tecnica, illustrando le proprie riserve sulla soluzione proposta e prospettando possibili approcci alternativi, come di seguito dettagliato.

2. Motivazioni di non ricevibilità della proposta OMISSIS basata sul modello belga

Omissis ritiene che la proposta formulata da OMISSIS non sia **ricevibile**, né sotto il profilo tecnico- realizzativo né sotto quello della coerenza con i principi regolamentari sin qui condivisi. Le principali motivazioni sono le seguenti:

- **Impraticabilità tecnica senza accordi CAMEL dedicati:** La realizzazione del blocco delle chiamate internazionali con CLI mobile, secondo il modello proposto, risulta tecnicamente complessa e attualmente non attuabile. Tale schema si basa infatti su presupposti di interoperabilità tra reti che richiederebbero l'implementazione di accordi CAMEL tra operatori. **Che ruolo gioca CAMEL in tutto ciò?** CAMEL, nella

variante **Home Network Routing (HNR)**, può essere utilizzato per instradare in maniera controllata le chiamate dei clienti in roaming e potenzialmente verificare l'autenticità del loro CLI. In una configurazione HNR, la chiamata originata dal roamer viene "richiamata a casa" – ovvero, invece di uscire direttamente dall'infrastruttura internazionale come chiamata qualsiasi, viene trasferita prima alla rete home tramite CAMEL, che può poi completarla verso la destinazione finale. Questo permette alla rete home di **intervenire sulla segnalazione e controllare il CLI**.

In pratica:

- Se la chiamata proviene davvero da un cliente in roaming su una rete estera che **supporta CAMEL**, allora tramite CAMEL HNR la chiamata viene gestita dall'operatore home, che può reinserire il numero chiamante corretto e autorizzare la presentazione del CLI (sapendo che è genuino).
- Se invece la chiamata arriva da una rete che **non supporta/invoca CAMEL**, oppure da una fonte non autenticata, il sistema potrebbe instradarla direttamente senza mostrare il numero (CLI bloccato)– impedendo così al truffatore di far comparire un numero falso.

In teoria, CAMEL potrebbe quindi essere una **misura di mitigazione**: consente di *"bloccare a distanza chiamate vocali fraudolente"* intercettandole via segnalazione SS7. Tuttavia, ci sono **limiti significativi** che ne riducono l'efficacia come soluzione generale al problema dello spoofing:

- **Copertura limitata**: non tutti gli operatori mobili nel mondo supportano CAMEL (specialmente CAMEL HNR completo). Anzi, molti operatori – in particolare fuori dall'Europa – non hanno mai implementato questa funzionalità, e **è molto improbabile che oggi investano per implementarla su reti 2G/3G legacy**. Quindi esisteranno comunque percorsi di chiamata da reti senza CAMEL su cui i controlli HNR non si attivano.
- **Necessità di accordi capillari**: anche tra operatori che supportano CAMEL, bisognerebbe assicurarsi che *tutti* abbiano accordi HNR attivi con *tutti* i partner internazionali rilevanti. Nella pratica attuale, **CAMEL HNR viene invocato solo in scenari specifici e non universalmente su tutte le chiamate**. Rendere obbligatorio l'instradamento home di ogni chiamata internazionale con CLI mobile nazionale richiederebbe un coordinamento e sforzo notevole tra decine di operatori.
- **Impatto sulle reti moderne**: la questione dello spoofing CLI riguarda soprattutto le chiamate voce tradizionali su rete circuit-switched (2G/3G). Con l'evoluzione verso il **VoLTE/VoWiFi e le reti 4G/5G**, le chiamate voce dei roamers diventano sessioni dati verso l'IMS dell'operatore di casa, il che *di per sé* elimina alcuni anelli deboli (la chiamata è già "ancorata" alla rete home e viaggia autenticata). Quindi, molti operatori puntano su soluzioni come l'**abbandono del 2G/3G roaming** a

favore del VoLTE roaming per mitigare lo spoofing, anziché investire in nuovi accordi CAMEL su vecchie reti.

- **Possibili disservizi e costi**: interventi come rimuovere/anonimizzare il CLI se non verificato via CAMEL potrebbero comportare che alcune chiamate lecite (ad esempio da reti dove CAMEL non è attivo temporaneamente) arrivino senza identificativo, confondendo gli utenti. Inoltre, richiedono modifiche ai gateway internazionali e ai nodi di segnalazione: *"un'abilitazione generalizzata di CAMEL HNR richiederebbe test e sviluppi significativi sia a livello di rete sia di sistemi IT (billing ecc.)"*, un investimento che molti operatori valutano poco giustificato.

In definitiva, **CAMEL può aiutare a distinguere le chiamate roaming genuine da quelle falsificate** (poiché solo le prime attiverebbero correttamente la logica CAMEL/HNR), rendendo possibile bloccare o filtrare le chiamate con CLI mobile italiano provenienti da fonti non autorizzate. Ma si tratta di un rimedio **parziale e in declino**: esso si applica solo sulle reti legacy che già lo supportano, e difficilmente verrà esteso a chi non l'ha implementato finora.

- **Contrasto con il principio di preferenza del blocco rispetto all'anonimizzazione:** La soluzione proposta da OMISSIS risulta altresì in contrasto con l'approccio di fondo che Omissis sostiene, **nonché con quanto previsto dalla Delibera 457/24/CONS**, la quale prevede espressamente che, in presenza di chiamate internazionali con CLI mobile nazionale non riconducibili a un utente effettivamente in roaming, si proceda al **blocco della chiamata**. Questo principio – volto a tutelare l'utente destinatario e la trasparenza della comunicazione – viene disatteso dalla proposta OMISSIS, che prevede di sostituire il numero chiamante con un'etichetta generica anziché impedirne del tutto la ricezione. Omissis considera tale scelta **inadeguata e inefficace**, poiché consente comunque il recapito della comunicazione, lasciando irrisolto il rischio di truffe e abusi. L'anonimizzazione non interrompe infatti l'azione fraudolenta, ma semplicemente ne nasconde il CLI, mentre il blocco la previene alla radice. In altri termini, **l'approccio OMISSIS privilegia la continuità della chiamata a scapito della sicurezza dell'utente**, posizione che Omissis non condivide e che giudica inappropriata rispetto agli obiettivi del tavolo tecnico.

3. Richiamo delle osservazioni del 31 marzo 2025 su implementazione graduale e rischi

Senza voler ripetere integralmente quanto già dettagliato nelle osservazioni trasmesse da Omissis in data 31 marzo 2025, si ritiene opportuno **richiamarne i punti salienti**, in particolare riguardo alla **necessità di un'implementazione per fasi** delle misure anti-spoofing e ai potenziali **rischi associati** a un'introduzione parziale. Omissis ha infatti evidenziato come una **applicazione limitata iniziale** delle regole di blocco potrebbe

comportare effetti indesiderati: ad esempio, l'attuazione di soli alcuni blocchi (come il filtro sulle chiamate con CLI fisso o su numerazioni non allocate) in una prima fase rischia di indurre i soggetti malintenzionati a **aggirare la misura** sfruttando le tipologie di chiamata non ancora sottoposte a controllo (ad esempio utilizzando **CLI mobili reali e attivi**, appartenenti a ignari utenti). Ciò non solo esporrebbe questi ultimi a potenziali disagi (dovendosi difendere da chiamate mai effettuate), ma potrebbe anche **compromettere la percezione dell'efficacia** dell'intervento regolamentare da parte dell'utenza: finché il blocco non copra anche le chiamate con CLI mobile, il pubblico potrebbe non ritenere "affidabile" il numero chiamante, vanificando in parte l'obiettivo di fiducia nello strumento.

Omissis ritiene che nella prima fase bloccare solo i numeri fissi con prefisso +390 entranti dall'estero è una soluzione chiaramente comprensibile, poiché consente di comunicare alle imprese del comparto ed ai cittadini che la numerazione fissa non può essere alterata e che le chiamate da numerazione fissa sono sicure, mentre una chiamata da numero mobile potrebbe essere ancora fraudolenta. Bloccare, già nella prima fase, una sola parte dei numeri mobili, non ha senso, perché - fino a che possono arrivare chiamate con CLI mobile falso - non si sarà portato alcun vantaggio all'utenza e agli operatori del settore e non si sarà risolto alcun problema. Omissis sarebbe dunque favorevole, se attuabile in tempi brevissimi, a una prima fase che preveda il solo blocco del CLI spoofing da numerazioni fisse, secondo gli schemi che sono stati illustrati dall'Autorità. In ogni caso, anche la soluzione del CLI spoofing mobile deve arrivare quanto prima, certamente ben prima di fine 2025. Si invita pertanto l'Autorità a tenerne conto nella definizione finale delle modalità attuative, privilegiando – se possibile – un avvio contestuale e completo delle misure di protezione sul CLI, oppure assicurando che le eventuali fasi intermedie siano di **brevissima durata** e accompagnate da adeguate cautele per evitare gli abusi nel periodo transitorio. *(Le osservazioni già fornite da Omissis con la nota del 31/3/2025 si intendono qui integralmente richiamate quali parte integrante della posizione associativa, pur omettendone la ripetizione dettagliata.)*

4. Proposta alternativa: blocco a carico dell'operatore ricevente con "colorazione" del traffico internazionale in ingresso

Nel corso della riunione del 1° aprile u.s., Omissis ha suggerito di esplorare soluzioni alternative che garantiscano ugualmente il contrasto alle chiamate spoofing, ma con un diverso riparto operativo. In particolare, si è proposta la valutazione di un modello in cui gli eventuali blocchi delle chiamate fraudolente siano posti **a carico dell'operatore ricevente** (ossia l'operatore che termina la chiamata verso l'utente destinatario finale). Tale approccio sarebbe supportato dall'**obbligo in capo all'operatore di frontiera** – ovvero l'operatore che introduce il traffico internazionale nella rete nazionale – di **"colorare" il traffico** in ingresso proveniente dall'estero. Per "colorazione" si intende l'apposizione di un marcatore o qualificatore nella segnalazione di rete, atto a indicare che la chiamata ha origine da un tronco

internazionale. In base agli approfondimenti compiuti in riunione, sembra a chi scrive che gli operatori di transito esteri siano in grado di "colorare" le chiamate inserite in rete dai medesimi per avvisare l'operatore di destinazione che si tratta di chiamata da rete estera e, così, far scattare i debiti controlli, lasciando invece impregiudicate le chiamate originate da rete nazionale.

Anzitutto il CLI mobile interessato potrebbe direttamente essere di titolarità dell'operatore mobile di destinazione (chiamata tra due utenti dello stesso operatore mobile) che quindi potrà facilmente fare le verifiche direttamente sui propri sistemi. Dall'altra, se fosse un CLI mobile di altro operatore, l'operatore mobile ha certamente possibilità di effettuare le verifiche su HLR necessarie e interrogare l'altro operatore circa lo status di roaming del CLI in questione con maggiore rapidità ed efficienza dell'operatore internazionale di transito. **Nel caso in cui l'operatore di destinazione sia un operatore di rete fissa**, questi potrebbe effettuare i **medesimi controlli oggi previsti in capo all'operatore di transito**, avendo comunque la possibilità tecnica di applicare le stesse logiche di verifica e di blocco. Si garantirebbe così una **copertura più ampia ed omogenea del sistema**, superando i limiti attuali della distribuzione rigida delle competenze, senza rinunciare all'efficacia dei controlli.

Una siffatta soluzione presenterebbe vari vantaggi: in primo luogo, **sfrutta le informazioni già disponibili all'operatore mobile ricevente** riguardo alle proprie numerazioni mobili (ad esempio lo stato di registrazione o roaming di un numero CLI di sua assegnazione), rendendo più semplice e accurata la distinzione tra chiamate lecite e spoofing senza dover ricorrere a interrogazioni esterne complesse. In secondo luogo, essa **distribuisce in modo più equilibrato le responsabilità** del controllo tra gli attori coinvolti: l'operatore di frontiera assolve al compito di segnalare la provenienza internazionale, mentre l'operatore di terminazione effettua il filtraggio finale basandosi sulle policy anti-spoofing comuni e sulle proprie evidenze di rete. Omissis invita pertanto l'Autorità a considerare con attenzione questa ipotesi, ritenendo che meriti adeguata analisi tecnica e di impatto, anche in un'ottica di **maggiore flessibilità operativa** e di salvaguardia delle chiamate legittime.

5. Sulle chiamate internazionali con CLI mobile provenienti da SIM M2M

Omissis ritiene opportuno segnalare un ulteriore profilo di criticità non esplicitamente considerato nella proposta tecnica sin qui discussa, ovvero il possibile utilizzo **fraudolento di SIM M2M (Machine to Machine)** per l'inoltro di chiamate internazionali con CLI mobile italiano. È noto che le SIM M2M, in base alla loro natura e classificazione, **non sono destinate a effettuare traffico voce**, bensì a scambiare dati tra dispositivi automatizzati (es. impianti di telelettura, dispositivi IoT, sistemi di allarme). L'eventuale ricezione di chiamate internazionali con CLI mobile associato a una SIM M2M rappresenta, in tal senso, **un evidente indicatore di anomalia e potenziale attività fraudolenta**, che meriterebbe un trattamento specifico nei filtri di blocco.Si suggerisce pertanto che, nella versione finale delle specifiche

tecniche, venga prevista una **verifica strutturale della tipologia di SIM associata al numero CLI mobile presentato**: qualora la numerazione corrisponda a una SIM M2M (secondo le informazioni disponibili al gestore mobile), la chiamata **dovrebbe essere automaticamente bloccata.** Una simile misura sarebbe in linea con il principio di **prevenzione dello spoofing a partire da indicatori oggettivi di incompatibilità d'uso** e contribuirebbe ad arginare ulteriori vulnerabilità del sistema.

Conclusione e richiesta

Alla luce di quanto sopra esposto, Omissis rinnova la propria collaborazione con l'Autorità ai fini di individuare soluzioni **efficaci, tecnicamente sostenibili e proporzionate** per il contrasto del CLI spoofing. Si confida che le criticità segnalate sulla proposta in esame vengano opportunamente valutate.

In particolare, **Omissis sottolinea l'importanza di privilegiare, a parità di efficacia e sicurezza nei controlli, quelle soluzioni che garantiscano tempi di implementazione più rapidi**. In un contesto di crescente allarme per l'utilizzo illecito del CLI e di forte pressione da parte dell'opinione pubblica e delle istituzioni, non è più sostenibile rimandare l'adozione di contromisure concrete e operative. Le aziende BPO-Contact Center rappresentate da Omissis subiscono quotidianamente il danno reputazionale e commerciale derivante da fenomeni che nulla hanno a che fare con il telemarketing legale. Si ribadisce che in assenza di un rapido ed efficace intervento, il comparto è a rischio e il Legislatore potrebbe adottare drastiche misure che chiudano il canale commerciale telemarketing. La soluzione al CLI spoofing, nei controlli che si sono sin qui discusse, rappresenta un indubbio vantaggio e una assoluta necessità sia per le aziende BPO e list provider che vivono di telemarketing, sia per la committenza, che si potrà serenamente affidare a tale canale, avendo certezza che - finalmente - le tutele del RPO saranno pienamente operative.

Per questo, ogni ritardo rischia di tradursi in conseguenze gravi sia per il comparto sia per la tutela degli utenti.

Certi della Vostra attenzione, si porgono distinti saluti.

Roma 07 Aprile 2025

Omissis
Distinti saluti,
Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Autorità per le Garanzie nelle Comunicazioni

Direzione tutela dei consumatori Omissis

agcom@cert.agcom.it

Omissis

Roma, 31 marzo 2025

Oggetto: Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS – Omissis.

Diamo seguito all'audizione del 27/03/2025 per trasmettere le nostre prime osservazioni circa il documento *"Draft di Proposta di soluzioni tecniche di blocco sullo spoofing del numero e normativa tecnica"* oggetto dell'audizione. Considerato il breve tempo concesso per l'analisi del documento, la complessità della tematica trattata e l'esigenza di garantire un'effettiva partecipazione agli operatori impattati dalle misure ivi proposte, ci riserviamo di inviare ulteriori commenti nel proseguo del procedimento istruttorio tuttora in corso avviato tramite la delibera n. 457/24/Cons.

Di seguito, riassumiamo i nostri commenti circa la proposta tecnica ricevuta soltanto alcuni giorni fa.

A. Riguardo i nuovi obblighi di notifica e reportistica che verrebbero introdotti a carico di alcuni soggetti autorizzati ai sensi dell'articolo 11 del CCE.

La proposta prevede l'introduzione di una nuova tipologia di soggetto autorizzato in Italia ai sensi dell'articolo 11 del CCE e l'introduzione di obblighi di reportistica, senza tuttavia specificare le modalità operative. Se abbiamo capito correttamente, ciò sarebbe funzionale alla soluzione proposta per bloccare le chiamate con CLI mobile italiano, che non ci sentiamo di poter condividere per le ragioni esposte nel proseguo di questo documento.

Ci riserviamo di formulare le nostre osservazioni in merito agli obblighi di notifica e reportistica una volta che avremo a disposizione tutte le informazioni necessarie per la loro valutazione. Ad es. chi sarebbe l'autorità italiana destinataria della notifica richiesta, quali informazioni occorrerà indicare e/o allegare a questa notifica e la modalità con la quale la notifica stessa dovrà essere gestita (piattaforma sidfors oppure piattaforma ROC o addirittura tramite una diversa modalità).

B. Riguardo la misura di bloccare le chiamate vocali internazionali in arrivo con un numero geografico/fisso nazionale E.164, salvo casi giustificati.

La proposta tecnica, a nostro parere, richiederebbe delle integrazioni:

a) aggiungere ulteriori casi di blocco, come di seguito riportato:

- Il CLI contiene un country code inesistente o non assegnato;
- Il CLI si presenta con il +39 seguito dal solo distretto nazionale.

b) chiarire che la normalizzazione del PAI ovvero le cd "Azioni Preliminari ai blocchi" si applicherebbero soltanto ai PAI italiani;

c) chiarire se lo Stato di San Marino avente indicativo distrettuale 0549 debba essere ricompreso nella casistica di *tromboning* quando il traffico in entrata si presenta come +390549 e, quindi, soggetto a blocco;

d) integrare la lista delle eccezioni che NON prevedono il blocco, come di seguito riportato nel testo in grassetto:

- Le chiamate dirette a roaming number nazionali.
- Le chiamate dirette a numerazioni mobili associate a servizi (es. segreteria telefonica).
- **le chiamate dirette ad un numero internazionale.** Da notare che questa eccezione al blocco sarebbe applicabile anche nello scenario di blocco di chiamate con CLI mobile italiano.

C. Riguardo la misura di bloccare le chiamate vocali internazionali in arrivo con un numero mobile nazionale E.164 come CLI dopo aver controllato e verificato che l'utente finale non sia in roaming all'estero, salvo casi giustificati.

Purtroppo, riscontriamo la proposta non solo complessa nella sua architettura tecnica e nei requisiti preliminari ma soprattutto mancante in aspetti tecnici essenziali per garantire la sua effettiva operatività, ad es.:

a) Manca la definizione dell'allungamento «sostenibile» del tempo di setup della chiamata causato dalla query;

b) Manca la valutazione dell'effetto che il tempo di set up allungato avrà sui timer innescati nelle reti mobili per il setup delle chiamate voce;

c) Manca la definizione del dimensionamento «sostenibile» delle connessioni per la gestione delle query con le API degli operatori mobili.

Aspetti che non appaino di poco conto sotto un profilo tecnico e che evidenziano quali siano alcune delle sfide tecniche della soluzione ipotizzata. Ci si chiede, in effetti, se la tecnologia 4G ed ancor di più la tecnologia 5G non consentano soluzioni più efficienti. È oramai un fatto consolidato che gli operatori mobili stiano abbandonando le tecnologie 2G e 3G.

Rappresenta, inoltre, una soluzione sproporzionata per gli operatori di transito alcuni di essi di piccole dimensioni.

Uno degli elementi cardine su cui si fonda la soluzione tecnica proposta dagli operatori mobili è l'utilizzo da parte degli operatori di transito degli archi di numerazione mobili non portabili assegnati dal Ministero (database o elenchi) per realizzare la soluzione. Come sappiamo però questi elenchi non riportano informazioni aggiornate, nonostante gli sforzi costanti del MiMIT. La soluzione proposta sarebbe dunque priva pure di solidità circa le informazioni ottenute in seguito alla consultazione dei database pubblici. Ipotizzare che nell'imminente futuro i diversi elenchi/database pubblici di numerazioni verranno aggiornati tempestivamente (da notare che l'aggiornamento dovrebbe essere REAL TIME per poter costituire una base solida di partenza) appare quanto meno altamente improbabile sulla base della nostra esperienza oltre ventennale nel settore. Valga come esempio che Omissis risulta ancora assegnataria di numerazione mobile pur non essendo un operatore virtuale da diversi anni.

In base alle informazioni di cui disponiamo, la maggior parte dei paesi europei non hanno previsto di bloccare e/o oscurare il CLI mobile nazionale chiamante (per le difficoltà tecniche di identificare una soluzione efficace) e paesi come la Spagna, che avrebbero già deciso di bloccare questa tipologia di chiamate, non ha tuttavia identificato ancora la soluzione implementativa.

Per queste ragioni riteniamo che la esperienza in Belgio meriti un approfondimento specifico da parte dell'Autorità.

La soluzione adottata in Belgio prevede per i clienti mobili in roaming internazionale la sostituzione temporanea del B Number con un Home Routing Number (HRN) che garantisce l'affidabilità del CLI mobile. La sostituzione del B Number con il HRN viene effettuata in segnalazione dall'operatore mobile nazionale proprietario del CLI mobile. L'HRN appartiene ad un arco di numerazione nazionale non portabile. Quindi gli operatori di transito nazionali, che ricevono sulle loro interfacce internazionali chiamate con B Number uguale allo HRN, non bloccano queste chiamate e trasmettono il CLI affidabile alla rete mobile proprietaria del blocco di numerazione HRN a loro assegnato dal Ministero. La rete mobile recipient effettua i controlli dovuti sullo HRN ricevuto e ripristina il vero B number per poter poi terminare la chiamata.

Sarebbe auspicabile, pertanto, identificare anche in Italia una soluzione tecnica secondo lo stesso approccio tecnico ovvero che gli operatori di transito ricevano sull'interfaccia internazionale le chiamate con CLI mobile già "targate" in modo chiaro, certo, e senza dilazioni di tempo al fine di consentire all'operatore di transito di trasportare la chiamata verso la rete domestica.

Gli operatori mobili italiani potrebbero 'sfruttare' il lavoro già fatto dai loro omologhi in Belgio nei confronti degli operatori degli altri paesi che garantiscono il roaming e non partirebbero da zero qualora occorresse aggiornare eventuali accordi di roaming. Questo in realtà è lo spirito che dovrebbe guidare l'attività regolamentare in Europa che in maniera armonizzata implementa soluzioni comuni per lo sviluppo del mercato e la tutela dei clienti finali.

Si chiede pertanto che l'Autorità integri l'istruttoria avviata con la delibera 457/24/Cons con le informazioni utili che otterrà da BIPT, il regolatore belga, in merito alla soluzione tecnica da loro implementata nonché circa l'esperienza che hanno maturato finora.

Infine, occorre definire il modello economico che verrà adottato per il ristoro agli operatori di transito dei costi sostenuti per l'implementazione delle eccezioni al blocco. È una tematica che l'Autorità non può più ignorare, soprattutto alla luce della soluzione tecnica proposta al settore. Per assurdo, gli utenti italiani potrebbero essere tutelati dal fenomeno del CLI spoofing sul mobile con le stesse misure e blocchi adottate per le chiamate con CLI fisso.
Ovviamente questa sarebbe una misura drastica, non desiderata, che avrebbe implicazioni negative per i clienti degli operatori mobili che sono in roaming all'estero. Non di meno, è un onere degli operatori mobili – e non degli operatori di transito – garantire il servizio di roaming che commercializzano. Implementare eccezioni al blocco dei CLI mobili italiani non può gravare in maniera sproporzionata sugli operatori di transito come invece gli operatori mobili stanno proponendo.
Ogni rete ha le proprie complessità. Le sfide delle reti mobili devono essere a carico di chi ha costruito le reti per operare in quello specifico mercato. Soggetti terzi che non operano nel mercato mobile non devono farsi carico della loro complessità tecnica perché hanno scelto di non entrare in quel mercato e devono rimanere fuori dalla gestione degli scenari mobili come quello del roaming.

Il compromesso tra i diversi interessi si trova nell'identificare una soluzione tecnica che permetta agli operatori di transito di non eseguire il blocco dopo una verifica del campo PAI mobile dei clienti in roaming "autoparlante", come accade per i CLI di rete fissa, poiché gli operatori di transito sono operatori di rete fissa e non operatori di rete mobile. Questo appare l'unico approccio in linea con il principio di proporzionalità e ragionevolezza che deve guidare l'attività regolamentare.

D. Ulteriori commenti circa le slides contenute nel documento "Draft di Proposta di soluzioni tecniche di blocco sullo spoofing del numero e normativa tecnica"

Slide n. 2 - Quadro e temi propedeutici generali per le soluzioni

- Testo attuale: L'obiettivo deve essere di aumentare la presenza e l'affidabilità del CLI visualizzato al cliente (da evitare l'anonimizzazione del CLI).
- Proposta di modifica: L'obiettivo deve essere di aumentare la presenza e l'affidabilità del CLI visualizzato al cliente (da evitare l'anonimizzazione del CLI) *fatte salve le scelte di visualizzazione esercitate dal chiamante.*
- Motivazione: si suggerisce di tenere in conto nella formulazione del testo che la funzionalità del Calling Line Identification Restriction (CLIR) deve comunque essere consentita al chiamante ai sensi della vigente normativa.

Slide n. 3 - Definizioni

CLI (calling line identity)

- Testo attuale: numero E.164, aderente al Piano di Numerazione Nazionale, univoco su base globale che identifica l'utente di origine della comunicazione ed è, in particolare, associato all'accesso della rete di origine a cui è attestato l'utente chiamante
- Proposta di modifica: per identificazione della linea chiamante si intendono i dati che consentono l'identificazione del numero da cui è possibile effettuare una chiamata o a cui è possibile effettuare una chiamata di ritorno.
- Motivazione: la definizione proposta è troppo restrittiva senza un'apparente motivazione poiché richiama il Piano di Numerazione Nazionale. Esistono dei CLI chiamanti e chiamati che pur non essendo aderenti al Piano di Numerazione Nazionale sono legittimi come ad es. i numeri di telefono di altri paesi. Inoltre, la definizione proposta identifica soltanto il caso di Network number/Network CLI/PAI ed esclude altri tipi di CLI come ad es. il caso del Presentation number.

Spoofing

- Onde evitare il proliferare di definizioni e fornire maggiore certezza giuridica, si suggerisce di sostituire il testo presente nella slide con la definizione riportata nella delibera 112/19/CIR che recita: *"Il CLI spoofing consiste nella pratica che consente alla parte chiamante, alla rete di origine e / o alla rete di transito di manipolare le informazioni contenute nel campo CLI con l'intenzione di ingannare la parte chiamata inducendola a pensare che la chiamata abbia avuto origine da un'altra persona, entità o, comunque, da altra linea."*

PAI (P-Asserted-Identity)

- Testo attuale: elemento informativo della segnalazione SIP (ITX VoIP) che contiene l'identità di origine della comunicazione certificata dall'operatore di origine ed

all'interconnessione, incluse le informazioni di presentazione o restrizione dell'identità verso il cliente chiamato. E' il cosiddetto CLI della chiamata.

- Proposta di modifica: elemento informativo della segnalazione SIP (ITX VoIP) che contiene l'identità di origine della comunicazione certificata dall'operatore di origine ed all'interconnessione, incluse le informazioni di presentazione o restrizione dell'identità verso il cliente chiamato. *E' il cosiddetto Network CLI o Network number* ~~CLI della chiamata~~.
- Motivazione: da un punto di vista tecnico esiste anche il Presentation CLI/Presentation Number/From che non identifica necessariamente l'identità della linea dell'origine geografica della chiamata.

Slide n. 4 - Pre requisiti generali

Punto 1

- Testo attuale: Tutti i Carrier Internazionali Autorizzati in Italia che ricevono traffico da rete di operatore estero per consegnarlo in Italia e che operano i blocchi devono dichiarare tale attività.
- Proposta di modifica: Tutti i Carrier Internazionali Autorizzati in Italia che ricevono traffico da rete di operatore estero per consegnarlo in Italia ~~e che operano i blocchi~~ devono dichiarare tale attività.
- Motivazione: capiamo che l'obbligo di notificare le proprie attività si applicherebbe ai Carrier Internazionali Autorizzati in Italia, indipendentemente dal loro grado di ottemperanza con il sistema stesso di blocco del traffico.
- Ulteriori richieste: chiarire chi sarebbe il destinatario della notifica e la modalità per realizzarla nonché le informazioni che occorrerà fornire (tramite la piattaforma sidfors oppure la piattaforma roc ?)

Punto 2

- Testo attuale: Tali operatori devono comunicare tempestivamente la cessazione dell'attività di «Carrier Internazionale Autorizzato in Italia» ad AGCOM ed agli operatori italiani (a questi ultimi con un preavviso di almeno 90 giorni fermo restando gli obblighi contrattuali tra le parti)
- Proposta di modifica: Tali operatori devono comunicare tempestivamente la cessazione dell'attività di «Carrier Internazionale Autorizzato in Italia» ad AGCOM ed agli operatori *mobili* italiani *firmatari dell'A.Q.* ~~(a questi ultimi con un preavviso di almeno 90 giorni fermo restando gli obblighi contrattuali tra le parti)~~
- Motivazione: fatto salvo quanto indicato al punto A. precedente, capiamo che l'A.Q. sarebbe funzionale alla proposta di soluzione tecnica per elencare i casi di eccezione al blocco delle chiamate vocali internazionali in arrivo con numero mobile italiano. In questa ipotesi di soluzione tecnica, non condivisa dalla scrivente, l'A.Q. sarebbe oggetto di negoziazione e disciplinerebbe la modalità di risoluzione/recesso da parte dei firmatari secondo quanto indicato nel documento ricevuto dall'Autorità. Appare pertanto prematuro determinare già che in caso di cessazione delle attività di Carrier Internazionale Autorizzato in italia il preavviso dovrà essere di almeno 90 giorni. Mal si comprende anche l'esigenza di prevedere un termine minimo per il preavviso. Si noti che la decisione da parte di una Carrier Internazionale Autorizzato in Italia di cessare la propria attività potrebbe essere adottata in un lasso di tempo incompatibile con un preavviso di ben 90 giorni.

Punto 5

- Testo attuale: AGCOM/Garante Privacy devono consentire esplicitamente la produzione di cartellini di traffico per le chiamate bloccate (in-effective).
- Si chiede di fornire chiarimenti circa questo prerequisito, ad es. quale sia la motivazione ed il contesto nel quale i cartellini di traffico verrebbero prodotti.

Distinti saluti.

Omissis

Firmato digitalmente da: Omissis
Data: 31/03/2025 14:44:49

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Autorità per le garanzie nelle comunicazioni
Centro Direzionale Isola B5
Torre Francesco
80143 NAPOLI

Direzione tutela dei consumatori

Att.ne del responsabile del procedimento
Ing. Giovanni Santella

Omissis
Invio tramite pec a agcom@cert.agcom.it

Oggetto: Consultazione pubblica di cui alla Delibera n. 457/24/CONS

Si trasmettono in allegato le osservazioni di Omissis in relazione alla proposta di soluzione tecnica per il contrasto dello spoofing del CLI in chiamate provenienti dall'estero, illustrata in sede di prima riunione del Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS, il 27 marzo u.s..

Cordiali saluti.

Omissis

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Posizione di Omissis in relazione alla proposta di soluzione comunicata da AGCom e illustrata in sede di Tavolo tecnico nella riunione del 27 Marzo 2025, ad integrazione dei propri contributi già inviati.

Quadro e temi propedeutici generali

Omissis concorda con le impostazioni alla base della stesura delle specifiche tecniche, in particolare con l'esclusione di soluzioni protocollari, come Stir-shaken, da considerarsi non efficaci allo scopo.

Definizioni

Si propone una piu' precisa definizione di Carrier Internazionale allo scopo di chiarire senza ambiguità gli ambiti soggettivi di responsabilità del nuovo quadro regolamentare.

Carrier Internazionale Autorizzato in Italia: qualsiasi operatore autorizzato in Italia, ai fini della consegna delle chiamate in Italia, interconnesso direttamente (per servizi di comunicazione fonia) con reti di operatori esteri non autorizzati in Italia.

Prerequisiti generali

Omissis concorda con il proposto processo che dovrà precedere l'implementazione tecnica dei blocchi delle chiamate con CLI contraffatto.

Blocchi (con CLI non mobili) che non richiedono query tra operatori

Tra le casistiche da bloccare (campo SIP PAI user part per l'interconnessione VoIP e CgPN per l'interconnessione TDM/ISUP) si ritiene debba essere aggiunta:

- +390XYZ, con XYZ non identificante uno dei distretti geografici previsti dal Piano di numerazione nazionale.

Blocchi (con CLI mobili) che richiedono query tra operatori

1. Prerequisiti

Omissis non ritiene necessaria, per maggiore trasparenza della disciplina, l'adozione di uno specifico Accordo quadro interoperatore, nella misura in cui AGCom auspicabilmente definisca un quadro regolamentare completo in materia.

2. Fasi

Omissis ritiene che, una volta definito l'elenco delle casistiche dei blocchi da mettere in atto (da parte dei carrier internazionali) riguardanti chiamate ricevute dall'estero con CLI non mobile, possa essere stabilita una pianificazione per l'attuazione tecnica di tali attività, sulla base delle analisi di fattibilità dei carrier stessi. (Fase 1)

Per quanto concerne le chiamate con CLI mobile, la pianificazione temporale degli interventi potrà essere stabilita a valle della redazione delle specifiche tecniche della soluzione, sulla base delle analisi di fattibilità di carrier internazionali ed operatori mobili. (Fase 2)

3. Rilevazione dello stato del CLI mobile

Omissis concorda con la struttura generale della soluzione. Ritiene tuttavia che debbano essere corretti alcuni dei criteri proposti per l'individuazione dei casi di blocco. In particolare, si propone che tali casi siano articolati in tre distinte categorie nel modo seguente:

Casi in cui l'operatore mobile risponde obbligatoriamente con "Blocco della chiamata":

(i) Numerazione chiamante non attiva sulla propria rete
(ii) Numerazione chiamante relativa a cliente registrato in Italia

Casi in cui l'operatore mobile risponde opzionalmente con "Blocco della chiamata":

(i) Numerazione chiamante relativa a cliente non registrato (es. terminale spento) (nota: la rilevazione di tale stato del terminale tipicamente richiede un interlavoro con la rete di accesso la cui fattibilità in tutti i casi (i quali spesso dipendono dalla durata del periodo di tempo decorso dallo spegnimento) è da approfondire e che potrebbe anche innescare fenomeni anomali su eventuali messaggi di reperibilità e annunci. Ciascun operatore potrebbe autonomamente ponderarne l'introduzione nei casi possibili)
(ii) Numerazione chiamante relativa a cliente registrato all'estero in 4G/VoLTE (nota: la rilevazione di tale stato introduce un grado di complessità realizzativa non indifferente relativa tuttavia a casistiche di spoofing che potrebbero probabilmente rivelarsi residuali. Ciascun operatore potrebbe autonomamente introdurre questa analisi in una fase successiva, anche sulla base degli effettivi riscontri operativi degli esiti delle procedure di blocco)

Casi in cui l'operatore mobile risponde opzionalmente con "Blocco della chiamata", nei soli casi in cui il chiamato sia un numero di un proprio cliente:

(i) Numerazione (CLI) individuata come sospetto spoofing sulla base di proprie rilevazioni
(ii) Numerazione (CLI) individuata come sospetta frode sulla base di proprie rilevazioni

(nota: il blocco delle chiamate sulla base di criteri autonomamente sviluppati dall'operatore dovrebbe essere consentito solo riguardo a chiamate indirizzate a propri clienti, rispetto ai quali l'operatore può esercitare correttamente la propria responsabilità)

4. Architettura funzionale

Omissis concorda con la definizione di una API standard a livello nazionale per l'interrogazione real-time delle reti mobili.

E’ auspicabile, se possibile, l’attuazione di una architettura ad hub delle VPN tra le piattaforme di operatori mobili e carrier internazionali per rendere piu’ efficiente l’esercizio della rete di connessioni utilizzate per l’interlavoro delle query/risposte.

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Spett.Autorità per le Garanzie nelle comunicazioni
Direzione tutela dei consumatori
alla cortese attenzione di
Dott. M. Carlomagno
Omissis

Omissis

Oggetto: Osservazioni Omissis relative al tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Gentile Autorità,

con la presente intendiamo rinnovare il nostro apprezzamento per la convocazione di un Tavolo Tecnico finalizzato a definire le modalità implementative delle misure tecniche per bloccare il fenomeno del CLI Spoofing, aperto ad un'ampia partecipazione di stakeholders interessati.

Stante la specificità tecnica delle soluzioni proposte nella documentazione allegata alla convocazione, Omissis prende atto delle valutazioni illustrate nel corso del Tavolo da parte degli operatori infrastrutturati integrati che le hanno elaborate e confida che queste possano effettivamente condurre ad una rapida e significativa riduzione del fenomeno del CLI spoofing, i cui impatti negativi sulla nostra clientela e più in generale su molti settori della commercializzazione di servizi ai clienti finali abbiamo già avuto modo di illustrare a Codesta Autorità in altre occasioni.

Proprio in considerazione della rilevanza e della sensibilità del fenomeno, auspichiamo che AGCOM definisca tempistiche di implementazione rapide, richiedendo agli operatori che saranno chiamati a darvi attuazione di dare priorità a questi interventi.

Riteniamo, inoltre, fondamentale che alle misure che saranno implementate siano associati degli indicatori di performance (KPI), mirati a verificarne l'efficacia in esito ad un'attenta e continua attività di monitoraggio. Ciò anche al fine di identificare con tempestività la necessità di apportare modifiche o aggiornamenti in luce dell'evoluzione tecnologica e/o di un mutato approccio da parte dei soggetti all'origine della pratica fraudolenta del CLI spoofing. A tal riguardo riteniamo pertanto che il solo numero di chiamate bloccate non rappresenti

un indicatore sufficiente per dar conto dell'efficacia delle misure, ma occorrerà ad esempio monitorare anche l'effettiva diminuzione della reclamosità dei clienti legata a chiamate collegabili a pratiche di CLI spoofing.

Restiamo a disposizione per qualsiasi ulteriore chiarimento e necessità di interlocuzione.

Cordiali saluti,

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Omissis

Spett.le

Autorità per le Garanzie nelle Comunicazioni
Direzione tutela dei consumatori

Inviata tramite PEC all'indirizzo: agcom@cert.agcom.it
Omissis

Oggetto: Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 4S7 /24/CONS- Osservazioni Omissis

Con la presente si forniscono le osservazioni di OMISSIS al "Draft di Proposta di soluzioni tecniche di blocco sullo spoofing del numero e normativa tecnica" (in seguito anche "Allegato I") pubblicato sul sito di codesta Autorità.

Occorre preliminarmente osservare che OMISSIS è un operatore fisso non integrato che non gestisce direttamente sulle proprie interfacce di rete la ricezione di chiamate vocali internazionali. Tali chiamate vengono quindi terminate sulla rete OMISSIS principalmente mediante gli accordi di interconnessione e transito sottoscritti con l'operatore Omissis.

In relazione alla proposta formulata dagli operatori infrastrutturati, integrati su rete fissa e mobile, che hanno partecipato al tavolo preliminare avviato da codesta Autorità, **la Scrivente concorda che le soluzioni da individuare debbano rispondere ad un criterio di sostenibilità ed efficacia.** Per tali motivi, si condivide che siano escluse soluzioni quali lo Stir-Shaken ed analoghe che per essere efficaci necessitano di implementazione in tutti i Paesi europei e che risultano eccessivamente complesse ed onerose da implementare.

Entrando nel merito delle proposte di cui all'Allegato 1, si rappresenta quanto segue:

1. OMISSIS concorda con gli scenari di blocco delle chiamate geografiche e non geografiche (diverse dalle numerazioni mobili) consegnate da operatori esteri che non rispettano le Raccomandazioni ITU in materia di numerazione (Racc. ITU-T E.164 ed E.157).

   Tale blocco dovrebbe già essere previsto dalla maggior parte degli operatori e, in tal senso, si comunica che la Scrivente già provvede a bloccare eventuali chiamate non conformi alle disposizioni di cui alla Raccomandazione ITU-T E.157.

   Si ritiene inoltre condivisibile la proposta emersa in sede di tavolo tecnico, di applicare il blocco anche alle chiamate da numerazioni "+39" senza un distretto associato e a quelle con *"Country code"* non assegnato in ambito internazionale.

2. Con riferimento al blocco delle chiamate geografiche e non geografiche (diverse dalle numerazioni mobili) provenienti dall'estero con rispetto delle Raccomandazioni ITU, si concorda con la proposta di cui all'Allegato 1, in quanto trattasi ad ogni modo di uso illecito delle suddette numerazioni.

3. In merito al blocco da applicare sulle chiamate entranti aventi come mittente numerazioni mobili nazionali, dal momento che la misura proposta incide esclusivamente sui «Carrier Internazionali Autorizzati in Italia» e sugli operatori mobili, allo stato attuale non si ritiene di fornire ulteriori osservazioni di merito. Ad avviso della Scrivente, è infatti interesse preminente degli operatori mobili implementare le misure di sicurezza che ritengono necessarie al fine di contrastare il fenomeno di CLI spoofing delle numerazioni mobili ad essi assegnate.
4. In merito al ruolo degli operatori chiamati, la Scrivente concorda che nessuna delle misure abbia impatto su tali operatori, così come precisato al Prerequisito Generale n.7 di cui all'Allegato 1. **Ad avviso della Scrivente è infatti onere dell'operatore originante verificare la correttezza del CLI trasportato in rete.** A tal fine, OMISSIS in qualità di operatore fisso provvede a bloccare eventuali chiamate con CLI modificato o usato impropriamente dai propri clienti.

Nell'ambito della prima riunione del tavolo tecnico plenario, tenutasi ieri, sono state inoltre proposte delle misure alternative a quelle di cui all'Allegato 1. **Tali misure, tuttavia, non sono ancora state declinate nel dettaglio e quindi necessitano di un approfondimento ulteriore nell'ambito delle future riunioni del tavolo tecnico per valutarne eventuali impatti sul mercato, quali ad esempio nuovi obblighi di implementazione e relative tempistiche.**

La Scrivente, pertanto, si riserva sin d'ora di integrare il proprio contributo sulla base della prosecuzione dei lavori del tavolo tecnico, nello specifico qualora dovessero emergere eventuali obblighi ed oneri a carico degli operatori chiamati.

Per eventuali comunicazioni si prega di far riferimento Omissis.

L'occasione è gradita per porgere i più cordiali saluti.

Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Omissis

Spett.le
AGCOM – Autorità per le Garanzie nelle Comunicazioni

Alla C.A della Direzione Tutela dei Consumatori

Via PEC: agcom@cert.agcom.it
Omissis

Oggetto: Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS – osservazioni di Omissis concernenti la riunione del 27 marzo 2025

Con comunicazione del 20.03.2025, AGCOM convocava la riunione in oggetto, per discutere di specifiche tecniche per la realizzazione del provvedimento in consultazione; contestualmente, AGCOM riconosceva la possibilità di inoltrare osservazioni scritte.

Omissis, facendo seguito a quanto sopra, ritiene opportuno richiamare di seguito alcune brevi riflessioni, peraltro già espresse nei precedenti contributi.

***

1) Evoluzione tecnica delle frodi e necessità di contromisure adeguate.

Si sottolinea in primo luogo l'importanza di aggiornare periodicamente le misure di contrasto al CLI *spoofing* ed alle tecniche frodatorie in genere.

Si ritiene infatti che qualsiasi sia la barriera tecnica che verrà posta, essa sarà oggetto di tentativi di elusione da parte dei frodatori, i quali escogiteranno puntualmente nuove modalità operative per "raggiungere" i consumatori in maniera fraudolenta.

Occorre dunque gestire tale scenario.

A tal scopo appare imprescindibile rivedere il testo al fine di prevedere il monitoraggio costante del settore, ed aggiornare conseguentemente le contromisure di cui trattasi.

Diversamente, ogni regolamentazione si troverà ad essere prima o poi obsoleta dinanzi al progredire delle tecniche utilizzate dai malintenzionati.

Ciò nell'ambito di una impostazione generale contraddistinta da un presupposto chiaro: l'onere, in capo ai Professionisti di settore, di adoperarsi per garantire la genuinità dell'identità chiamante, quale elemento minimo di diligenza professionale.

***

2) Necessità di maggiore tutela nel caso di numerazioni sensibili.

In secondo luogo, Omissis. sottolinea nuovamente la pericolosità dello *spoofing* che realizza la "clonazione" dei numeri di enti ritenuti generalmente affidabili, come Forze dell'Ordine, Istituzioni, filiali di Banca, Compagnie Assicurative, etc.

Tale tecnica consente ai truffatori di fingersi "rappresentanti" dei soggetti menzionati, ottenere in tal modo la fiducia dei consumatori e carpire i loro risparmi in maniera fraudolenta.

Alla luce di ciò, si sottolinea l'importanza di proteggere tali numeri in maniera rafforzata, con accorgimenti che non li rendano, in nessun caso, clonabili. Si auspica dunque lo studio di misure tecniche in tal senso.

***

Per tutto quanto non espressamente trattato, si rimanda ai precedenti scritti Omissis.

Con riserva di ulteriori contributi, si rimane a disposizione dell'Autorità per ogni evenienza.

Distinti saluti.

Omissis

Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Autorità per le Garanzie nelle Comunicazioni (AGCOM).
Centro Direzionale, Isola B5
80143 Napoli.

Inviata mezzo PEC agcom@cert.agcom.it

Oggetto: Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Omissis

DICHIARA

PRIMO.- In relazione alla proposta tecnica definita dal tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS, ringraziamo l'opportunità di comunicarle la posizione di Omissis.

SECONDO.- Riteniamo appropriata la proposta di limitare l'intervento normativo alle chiamate internazionali in entrata, senza includere il traffico strettamente nazionale. La maggior parte delle pratiche scorrette si verifica nelle chiamate internazionali ed esistono già regole e strumenti per controllare le chiamate nazionali. Inoltre, gli strumenti che potrebbero essere applicati in relazione

alle chiamate nazionali sono estremamente complessi e la loro introduzione ritarderebbe inutilmente un intervento urgente.

TERZO.- Per quanto riguarda la soluzione proposta per bloccare le chiamate in roaming internazionale, e quindi con numeri mobili, riteniamo che la proposta sia eccessivamente complessa e che esistano misure più semplici, rapide ed efficaci per queste chiamate, come spiegheremo ora.

QUARTO – La soluzione proposta è molto complessa. La soluzione richiede uno sviluppo informatico complesso e costoso. Per di più, la soluzione proposta richiede che tutti gli operatori con interconnessioni internazionali realizzino sviluppi informatici. Si tratta di una soluzione molto inefficiente se si considera il sistema nel suo complesso. Gli operatori italiani con punto di interconnessione internazionale hanno spesso un'attività molto piccola in Italia, come nel caso di Omissis, il che comporta un onere sproporzionato. Sembra più ragionevole che gli operatori italiani che beneficiano del roaming (gli operatori di telefonia mobile) debbano sostenere la maggior parte dell'onere di controllare i CLI di telefonia mobile presumibilmente in roaming.

La soluzione richiede molto tempo per essere implementata. Poiché si tratta di una soluzione con uno sviluppo informatico impegnativo e deve essere sviluppata in parallelo da un gran numero di operatori, molti dei quali con un'attività locale ridotta, l'implementazione da parte di tutti gli attori richiederà inevitabilmente un lungo tempo di attuazione. L'esperienza nell'implementazione di questo tipo di soluzione, lo dimostra. In Irlanda, il regolamento in tal senso è stato approvati nell'aprile 2024, ma non entrerà in vigore prima del marzo 2026 (due anni per l'attuazione).

Infine, si tratta di una soluzione con un orizzonte di applicazione limitato nel tempo. Con la continua implementazione delle reti CAMEL e VoLTE, Omissis non prevede che gli operatori ricevano in futuro alcuna chiamata mobile illegittima sul loro gateway internazionale. Riteniamo quindi che il costo di progettazione, implementazione e manutenzione di una soluzione di “controllo del roaming” sarebbe inutilmente elevato per i limitati benefici che porterebbe.

QUINTO. Omissis ritiene che la soluzione più semplice ed efficace per ridurre l'impatto dello spoofing mobile consista nell'anonimizzazione del CLI mobile da parte degli Operatori italiani con punto di interconnessione internazionale. Ad esempio, se una chiamata con CLI "+393" entrasse nel gateway internazionale dal Italia da un altro paese, gli operatori nasconderebbero il CLI in modo che il chiamato in Italia vedesse una chiamata anonima. Nessuna di queste chiamate verrebbe bloccata. Ciò non richiederà sviluppi lunghi e complessi e potrebbe fornire una soluzione efficace a breve termine, migliorando la protezione dei clienti.

A più lungo termine, con il passaggio delle chiamate mobili a VoLTE e la configurazione del routing CAMEL Home da parte degli operatori mobili per le chiamate non VoLTE, garantiranno che gli Operatori italiani con punto di interconnessione internazionale non ricevano chiamate fraudolente dalle reti internazionali.

In conclusione, riteniamo che un approccio pragmatico al grave problema dello spoofing raccomandi misure efficaci ma semplici da attuare, in modo che possano essere implementate il prima possibile. Nel caso del CLI mobile in roaming, l'esperienza internazionale dimostra che soluzioni complesse come quella in esame possono richiedere due anni per essere implementate da tutti gli operatori (come nel caso dell'Irlanda). Al contrario, soluzioni come quella che proponiamo possono essere implementate in un periodo di tempo molto più breve, come un semestre (Belgio).

28 aprile 2025

Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

TAVOLO TECNICO SPOOFING

Considerazioni Omissis a proposta di specifiche tecniche

- Ringraziamo l'Autorità per l'avvio del tavolo tecnico e per la evidente volontà di trovare una soluzione efficace ad un problema che ha raggiunto dimensioni ormai intollerabili per i cittadini e che risulta dannoso per gli operatori corretti.
- In termini generali, ci sembra che la proposta posta in consultazione sia idonea ad affrontare le diverse casistiche di chiamate con prefisso italiano ma provenienti dall'estero, che a quanto emerso nel tavolo tecnico rappresentano la quasi totalità (il 98% circa) delle chiamate attualmente oggetto di spoofing.
- Con riferimento alle fasi di adozione degli interventi, la proposta in consultazione prevede che le misure di blocco siano applicate prioritariamente sui numeri diversi dai mobili (non standard ITU, fissi geografici e non) e solo in una seconda fase sui numeri mobili.
- Le evidenze ci dicono d'altra parte che la quasi totalità delle chiamate moleste (es. il 90% delle segnalazioni ricevute da Omissis) provengano da numeri mobili non richiamabili; riteniamo pertanto fondamentale che gli interventi riguardino con un grado elevato di priorità tali numeri.
- Auspichiamo pertanto che il blocco dei numeri mobili, insieme a quello dei numeri fissi e non standard ITU, sia implementato immediatamente a valle della delibera dell'Autorità e già entro la metà dell'anno.
- Quantomeno, riteniamo fondamentale che siano attuate fin da subito e contestualmente alle misure di blocco dei numeri diversi da mobili le misure relativa ai numeri mobili non assegnati. Per tali numeri, a quanto comprendiamo sulla base della proposta tecnica discussa al Tavolo, si prevede una attività di controllo/blocco in capo ai carrier internazionali sulla base di informazioni note ex ante (es. l'assegnazione o meno del numero). Il processo appare sostanzialmente analogo a quello relativo ai numeri diversi dai mobili (in cui i carrier internazionali bloccano numeri inesistenti) e ci sembra ragionevole, quindi, che l'adozione dei due set di misure segua tempistiche analoghe.
- Si potrebbe successivamente implementare la misura di blocco dei numeri mobili assegnati ma oggetto di spoofing, che a quanto capiamo prevede scambi di informazioni in tempo reale tra carrier internazionali ed operatori nazionali (es. su roaming) e quindi è ragionevolmente più complessa da finalizzare.
- Con riferimento infine alla possibilità, emersa nel tavolo tecnico, di futuri aumenti della casistica, oggi numericamente limitata, di chiamate spoofing che nascono direttamente in Italia su rete VOIP e senza transito attraverso i carrier internazionali, riteniamo cruciale il ruolo dell'Autorità di sistematico controllo su tutti gli operatori telefonici relativamente al rispetto della normativa nazionale sul divieto di alterazione del numero telefonico.

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Spettabile
AGCOM
Direzione Tutela dei Consumatori
Centro Direzionale, Isola B5 – "Torre Francesco"
80143 – Napoli
c.a.
Ing. Giovanni Santella
Responsabile del procedimento

Inviata tramite posta elettronica (PEC) all'indirizzo: agcom@cert.agcom.it

Omissis
Omissis

Oggetto: Consultazione pubblica di cui alla delibera n. 457/24/CONS – Osservazioni di Omissis rispetto alle soluzioni individuate dal Tavolo Tecnico preliminare

Con delibera 457/24/Cons Codesta Autorità ha proposto l'adozione di alcune misure per garantire la trasparenza a tutela degli utenti finali rispetto alle chiamate con CLI modificato sottoponendole a consultazione pubblica al fine di raccogliere le osservazioni dei soggetti interessati.

Alcune di queste misure sono relative alla gestione delle chiamate vocali internazionali in arrivo direttamente sulle interfacce internazionali degli operatori. Al contempo lo Schema di Provvedimento allegato alla suindicata delibera riconosceva esplicitamente la necessità *" le misure adottate non compromettano la gestione delle legittime chiamate vocali internazionali in arrivo o non blocchino le eccezioni consentite a livello nazionale"*

L'Autorità nell'ambito della suddetta consultazione pubblica, tuttora in corso, ha inoltre proposto di definire le specifiche tecniche relative l'implementazione delle misure proposte nell'ambito di uno specifico tavolo tecnico. In attesa dell'approvazione definitiva delle misure è stato contemporaneamente avviato un tavolo tecnico preliminare nell'ambito del quale gli operatori

infrastrutturati integrati su rete fissa e mobile (TIM, Wind Tre, Vodafone Italia, Fastweb, Iliad) hanno formulato alcune proposte di specifiche tecniche sottoposte dall'Autorità a consultazione pubblica.

Di seguito si forniscono le osservazioni di Omissis rispetto a quanto indicato nella presentazione ricevuta con comunicazione del 20 marzo u.s. nonché a quanto emerso nel corso delle riunioni del 27 marzo e 3 aprile u.s. Le osservazioni saranno formulate seguendo l'ordine della suindicata presentazione. Nel presente contributo verranno inoltre forniti ulteriori dettagli rispetto alla proposta alternativa formulata da Omissis nel corso dell'audizione del 27 marzo.

1. Osservazioni rispetto alla proposta formulata nel Tavolo Tecnico Preliminare

SLIDE 2 - Quadro e temi propedeutici generali per le soluzioni

Nella Slide 1 vengono indicati gli obiettivi alla base delle soluzioni proposte, tra cui, "**aumentare la presenza e l'affidabilità del CLI visualizzato al cliente (da evitare l'anonimizzazione del CLI)".**

Sebbene si condivida la necessità di aumentare l'affidabilità del CLI, obiettivo posto alla base dell'azione regolamentare, si ritiene che l'anonimizzazione del CLI possa essere applicata in maniera residuale e complementare per quelle casistiche per le quali non si hanno elementi sufficienti per classificare il traffico come illegittimo e dunque procedere al blocco. Un simile orientamento sarebbe peraltro in linea con quanto proposto al comma 3 art 8 dello Schema di Provvedimento in base al quale "*Gli operatori garantiscono che le misure adottate non compromettano la gestione delle legittime chiamate vocali internazionali in arrivo o non blocchino le eccezioni consentite a livello nazionale*". L'anonimizzazione delle chiamate è inoltre una misura prevista dalla Raccomandazione ECC (23)03 ed attuata in diverse nazioni europee (tra le quali Belgio, Germania, Spagna) per contrastare il fenomeno del CLI spoofing.

L'anonimizzazione di una chiamata, difatti, contribuisce di per se a limitare il fenomeno dello spoofing e delle truffe telefoniche considerando che l'utente telefonico è portato a non rispondere a chiamate con CLI anonimo e, in ogni caso, tali chiamate non potrebbero avere alcun

seguito non essendo presentato all'utente alcun CLI da ricontattare/aggiungere su applicazioni di messaggistica ai fini di una eventuale truffa.

Omissis concorda inoltre con la necessità di misure armonizzate e mandatorie a livello UE e globale per la definizione di regole sul CLI spoofing in grado di contrastare efficacemente le varie tipologie di spoofing massimizzandone l'efficacia in termini di tutela della clientela finale.

A tal riguardo, proprio al fine di garantire il massimo livello di armonizzazione a livello implementativo si ritiene utile anche guardare alle *best practices* a livello europeo, ciò al fine di individuare soluzioni efficaci sia sotto il profilo dei costi che delle tempistiche implementative. A parere della scrivente si dovrebbero infatti privilegiare **soluzioni semplici e veloci da implementare, in grado di garantire tempestivamente ed efficacemente le tutele necessarie agli utenti finali garantendo al contempo un impatto contenuto in termini di costo sugli operatori chiamati ad attuarle.**

SLIDE 3 (Definizioni)

Nella slide 3 viene proposta la definizione di "Carrier Internazionale Autorizzato in Italia". Tale definizione, non presente all'interno del Codice delle Comunicazioni, può dar adito a fraintendimenti: non si tratta, difatti, come lascerebbe intendere la definizione, di un nuovo soggetto giuridico ma di un operatore che opera a livello nazionale in conformità alle regole del codice che ha anche funzione di transito internazionale. Sarebbe pertanto più corretto parlare di **Operatore Autorizzato in Italia con interconnessioni internazionali.**

SLIDE 7- 11 - Blocchi con CLI mobili

La scrivente non condivide la soluzione proposta per il blocco delle chiamate provenienti su interfacce internazionali con CLI mobile nazionale presentata nelle SLIDE 7-11.

Nello specifico, secondo la soluzione proposta, i cosiddetti "Carrier internazionali Autorizzati in Italia" ogniqualvolta ricevono una chiamata internazionale sulle proprie interfacce dovrebbero:

1) bloccare la chiamata nel **caso di numerazione Mobile appartenente ad archi di numerazioni mobili (in decade 3) NON assegnati da MIMIT ad alcun operatore mobile** (in base alle informazioni contenute nel Data base del MIMIT)
2) nel caso di **numerazione Mobile appartenente ad archi di numerazioni mobili (in decade 3) assegnati ad un operatore mobile**: Identificare l'operatore sulla cui rete è configurato il numero ed interrogare l'operatore mobile il quale, verificato lo stato della numerazione (se in roaming o meno) fornisce un risposta di blocco/non blocco della chiamata. Si evidenzia che nella soluzione proposta l'operatore mobile fornisce una risposta di blocco della chiamata non solo nel caso di numerazione non attiva sulla propria rete ma anche nei casi di numerazioni gestite da parte di altri operatori. Ciò implica un rischio di blocco di chiamate legittime nel caso di un mancato aggiornamento del database MNP o del Database del MIMIT. A tal riguardo si evidenzia come la stessa Omissis abbia più volte segnalato inesattezze rispetto ai dati contenuti del database MNP.

La soluzione proposta prevede, inoltre, una serie di attività propedeutiche da svolgere per una corretta implementazione della stessa. Nello specifico gli operatori mobili dovranno **definire e fornire una API uguale per tutti per la query necessarie alla verifica delle chiamate da bloccare/non bloccare.** I cosiddetti "carrier internazionali" dovranno invece stabilire una **connessione privata IP sicura con ognuno degli operatori mobili destinatari delle query**. A tal fine dovranno essere stipulati specifici accordi bilaterali.

La soluzione sopradescritta, a parere di Omissis, comporta una eccessiva complessità che inevitabilmente causerà un allungamento delle tempistiche necessarie perché tutti gli operatori riescano ad adeguarsi, con conseguente danno per la clientela finale.

Come indicato nella presentazione, inoltre, all'interno della soluzione proposta risultano ancora da approfondire due tematiche essenziali ai fini di una sua corretta valutazione in termini di efficacia e sostenibilità:

1) L'impatto che le query avranno sul tempo di setup della chiamata: a dispetto del fatto che le numerazioni mobili in roaming rappresentano una parte esigua rispetto al totale delle numerazioni, le query necessarie per verificare lo stato delle suddette numerazioni

potrebbero determinare un impatto su tutte le chiamate gestite sulle interfacce internazionali di cui si dovrà necessariamente tener conto prima di procedere ad una sua approvazione definitiva

2) L'operatore di transito dovrà dotarsi di un numero di connessioni per ciascuno degli operatori assegnatari di numerazioni mobili: tale soluzione comporterà una significativa complessità di gestione sia nella fase iniziale di implementazione sia successivamente: non è chiaro, difatti, se la misura mira ad imporre in capo all'operatore di transito l'onere di individuare sul mercato tutti gli operatori con i quali sorgerebbe poi un obbligo a negoziare. Se fosse questo il caso la misura appare eccessivamente gravosa, non sostenibile e non condivisibile da Omissis. Si consideri inoltre che basterebbe un cambiamento proprietario/societario di un qualsiasi soggetto coinvolto per determinare la necessità di modificare una delle connessioni implementate. Ciò fa si che la misura richieda una continua opera di aggiornamento rispetto ai soggetti presenti. In aggiunta, non sempre l'operatore, per ragioni di tutela della sicurezza della propria rete, può inserire nello switch una connessione diretta con un sistema esterno (ad esempio con il server di un operatore mobile). E' questo il caso di un operatore transnazionale come Omissis che ha una rete IMS a livello europeo alla quale, per ragioni di sicurezza non si connettono sistemi esterni: ciò implica la necessità di coinvolgere una terza parte per implementare le query richieste dalla soluzione proposta, con ulteriore aggravio dei costi, o di dover sottoscrivere un accordo commerciale con un operatore MNO per la gestione dei blocchi.

Al fine di evitare le suesposte complessità e di garantire maggiore armonizzazione nella lotta contro lo spoofing, la scrivente suggerisce, come già indicato nella propria risposta alla consultazione pubblica di cui alla delibera 457/24/CONS e nel corso della riunione plenaria del Tavolo Tecnico tenutasi in data 27 marzo u.s. di analizzare soluzioni già implementate con successo in altri parsi europei, quale quella belga, basate sull'utilizzo dell'HRN (Home Routing Number).

2. Soluzioni di contrasto al CLI spoofing basate su HRN

Le misure per contrastare il CLI spoofing adottate in Belgio

Le misure per contrastare il fenomeno del CLI spoofing sono state adottare in Belgio con il Royal Decree del 12 maggio 2024[1] . Il Regio Decreto, in linea con quanto indicato nella raccomandazione ECC (23)03, si basa sul principio che è generalmente ingiustificabile che le chiamate provenienti dall'estero siano associate a numeri telefonici belgi proponendo misure di blocco per le chiamate vocali internazionali in entrata con numeri telefonici nazionali "E.164" che si sospetta siano stati falsificati. E tuttavia, riconoscendo che non tutto il traffico internazionale in arrivo con un numero geografico/fisso nazionale E.164 è illegittimo ha indicato specifiche eccezioni che riguardano (si veda l'art 4 del regio decreto):

- chiamate effettuate utilizzando la linea internet: vengono citate a tal riguardo i casi di applicazioni quali Teams che consentono di utilizzare i numeri telefonici geografici in mobilità. Si cita come esempio specifico il caso di un'azienda che utilizza quotidianamente i Teams in Belgio, ma il cui dipendente effettua occasionalmente chiamate dall'estero per motivi di servizio;
- i servizi di teleconferenza, i servizi di assistenza clienti e i servizi di marketing telefonico diretto, se sono offerti come applicazione cloud (cfr. scenario 4 della citata raccomandazione CEE n. 23(03) del 28 novembre 2023). La natura dematerializzata di questi servizi fa sì, a parere del regolatore belga, che il legame con la posizione geografica del numero chiamante non sia più considerato un elemento essenziale.

Con riferimento alle numerazioni mobili, il regolatore belga, al fine di contemperare la necessità di individuare una soluzione efficace sotto il profilo della lotta allo spoofing con l'esigenza di non

[1] Cfr Royal Decree on spoofing | BIPT

gravare gli operatori con soluzioni eccessivamente onerose ha deciso di adottare la strategia dell'"**Home Routing**".

Tale soluzione, che **risulta essere in linea con le modalità di instradamento già oggi usate dagli operatori mobili per la gestione delle chiamate in roaming**, è stata discussa e condivisa nell'ambito di AGORIA, la piattaforma belga di cui sono membri la maggior parte degli operatori, attivi in diversi segmenti di mercato Omissis.

Modalità di gestione delle chiamate in roaming

Quando un cliente di un operatore mobile è in roaming, l'HLR (Home Location Register della rete domestica [2]) e il VLR (Visitor Location Register della rete in roaming [3]) vengono aggiornati di conseguenza.

Quando un **utente in roaming riceve una chiamata nazionale sul proprio cellulare** (chiamate Inbound) questa viene instradata verso la rete domestica. Sulla base delle informazioni contenute nell'HLR, il VLR della rete in roaming viene informato della chiamata in arrivo e assegna un numero temporaneo, l'MSRN, e la rete domestica sostituisce il B number con l'MSRN e "inoltra" la chiamata. Una volta raggiunta la rete di roaming, la chiamata viene inoltrata al cellulare in roaming.

Quando un utente effettua una chiamata dal suo cellulare in roaming le chiamate possono essere instradate secondo due principi:

- **Local routing** (logica di instradamento predefinita nelle reti 2G): in tale scenario la rete di roaming instrada la chiamata secondo la propria logica di instradamento.
- **Home Routing**: in tale scenario la chiamata viene prima instradata verso la rete domestica e l'operatore domestico instrada la chiamata verso la destinazione finale. L'instradamento

[2] Se un cellulare è in roaming, l'HLR della rete di origine memorizza le informazioni richieste dalla rete in roaming

[3] Se un cellulare è in roaming, il VLR della rete di roaming memorizza le informazioni richieste dalla rete di origine. Questo registro non memorizza il numero di telefono ma l'IMSI (International Mobile Subscriber Identity) del cellulare.

verso la rete domestica è un servizio CAMEL[4] che deve essere supportato sia dalla rete domestica che da quella di roaming. Tale modalità di instradamento è iniziata a diventare la logica di instradamento predefinita per il 3G **ed è la logica di instradamento predefinita per il 4G e 5G.**

Applicazione di soluzioni basate su HRN per la gestione di CLI spoofing proveniente da numerazione mobili

Le modalità con le quali già oggi gli operatori mobili gestiscono le chiamate dei propri utenti in roaming possono essere facilmente utilizzate per bloccare, in maniera efficace e veloce, il fenomeno del CLI spoofing proveniente da numerazioni mobili.

Secondo quando proposto nella Schema di Provvedimento sottoposto a consultazione pubblica gli operatori dovrebbero bloccare dalle proprie interfacce internazionali tutte le chiamate con CLI mobile nazionale con l'eccezione delle chiamate effettuate dagli utenti in roaming.

Tale informazione, come si è avuto modo di evidenziare nella propria risposta alla sopra citata consultazione, non è nella disponibilità dell'operatore fisso ma esclusivamente dell'operatore mobile.

La soluzione proposta dal Tavolo preliminare, basata su query API attraverso cui verificare lo stato della numerazione appare, come già indicato, complessa da implementare, richiedendo una fase di attività propedeutiche estremamente difficoltosa sia da un punto di vista tecnico che negoziale. A ciò si aggiunga che alcuni dei requisiti fondamentali per valutare l'efficacia della soluzione stessa sono, ad oggi, ancora da analizzare (tempi di set up della chiamata, sostenibilità di implementare connessioni dedicate per ciascun operatore mobile, necessità di identificare in maniera esaustiva tutti i soggetti con cui i carrier internazionali sarebbero obbligati a sottoscrive un accordo, tematiche legate alla sicurezza delle reti). **Ciò rende necessariamente lunghi ed incerti i tempi di implementazione della soluzione, alla quale risultano inoltre associati significativi costi di implementazione e mantenimento. A tal riguardo non risulta chiaro se vi siano costi connessi**

[4] Customised Applications for Mobile networks Enhanced: Un insieme di servizi/applicazioni definiti principalmente per supportare la funzionalità di roaming (avanzata). L'Home Routing rientra tra I CAMEL.

all'attività di query richiesta per la verifica delle chiamate in roaming. Si evidenzia sin da ora che tali eventuali costi non potranno essere posti a carico dell'operatore di transito.

La soluzione basata sull'Home Routing, di contro, utilizza logiche già presenti per la gestione delle chiamate in roaming che possono essere mutuate con estrema facilità per la gestione del fenomeno del CLI spoofing: se viene avviata una chiamata da un cellulare in roaming, il VLR interroga l'HLR e viene assegnato un numero temporaneo, l'HRN, mentre il B number viene sostituito dall'HRN e la chiamata viene instradata verso la rete domestica. Una volta raggiunta la rete domestica, l'HRN viene sostituito dal numero composto e la chiamata viene instradata verso la destinazione finale.

Con l'Home Routing il numero di destinazione è dunque un HRN. Generalmente, i range di numeri HRN sono conosciuti solo dalla rete domestica. Per evitare il blocco di queste chiamate tali range dovranno essere comunicati a tutti gli operatori di transito. Solo in rari casi (assenza di accordo CAMEL), l'Home Routing non viene applicato. Per evitare il blocco di chiamate potenzialmente legittime garantendo allo stesso tempo che lo spoofing dall'estero non sia possibile si dovrebbe applicare una misura aggiuntiva di anonimizzazione delle chiamate in entrata dall'estero con un CLI nazionale.

In definitiva una soluzione basata sull'HRN appare:

- in linea con i principi della proporzionalità, efficienza e certezza dell'azione regolamentare in quanto garantisce la rapida applicazione delle misure di contrasto al fenomeno del CLI spoofing a tutela dell'utente finale rendendo al contempo sostenibile la soluzione per tutti gli operatori presenti sul mercato;
- semplice da implementare sia per gli operatori mobili che per gli operatori di rete fissa in quanto:
    - basata su logiche già oggi utilizzate per la gestione delle chiamate in roaming
    - non richiede la stipula di alcun accordo tra operatori di transito ed operatori mobili né tantomeno la predisposizione di connessioni dedicate per le attività di query
- in grado di tutelare la gestione del traffico legittimo tramite l'anonimizzazione dei casi residuali di traffico per il quale gli operatori non hanno stipulato un accordo CAMEL

- non impattare in alcun modo sui tempi di set up della chiamata che non andranno modificati

Si chiede pertanto che Codesta Autorità, prima di procedere all'approvazione della soluzione definitiva, voglia svolgere un ulteriore approfondimento relativamente a soluzioni alternative rispetto a quella indicata a conclusione del Tavolo Preliminare, basate su logiche già conosciute ed in parte implementate dagli operatori, quale quella basata sull'HRN.

Restando a disposizione per qualsiasi ulteriore chiarimento o informazione dovesse ritenersi necessaria si inviano Cordiali saluti

Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis.

Contributo al tavolo tecnico

Omissis
Oggetto: R: Delibera n. 457/24/CONS - Comunicazione di convocazione riunione

Omissis
Buonasera,

come richiesto, facciamo seguito agli approfondimenti relativi al tavolo in oggetto per condividere le osservazioni di Omissis sulla soluzione presentata.

A) Relativamente al punto 1.iii della slide 9 della soluzione proposta si riporta quanto segue.
Per l'operatore assegnatario della numerazione (verificata dal Carrier) non è detto che un Cliente mobile registrato all'estero in 2G/3G sia in un Paese dove è effettivamente presente una rete di accesso radio 2G/3G. Nel caso già in essere dell'Australia (dove gli operatori locali hanno dismesso le reti legacy 2G/3G e garantiscono copertura radio solo 4G) le SIM in roaming eseguono un combined attach che, al fine di garantire alcuni servizi (quali, ad esempio, gli SMS), ha l'effetto di registrare su HLR un VLR address come se il Cliente fosse registrato 2G/3G. Ne consegue che non sempre sarà possibile per l'operatore assegnatario della numerazione avere contezza del reale scenario in cui opera la SIM all'estero e pertanto discriminare se agire con un blocco obbligatorio o facoltativo : 1 iii) o 2 i).

Potrebbe ad esempio presentarsi lo scenario in cui si lascia passare una chiamata con il numero spoofato del Cliente in Australia che, avendo solo copertura 4G, non sarebbe dovuta entrare su interconnessione con carrier internazionale.
Per capire realmente se il Cliente è registrato o meno su una rete di accesso 2G/3G è necessario anche verificare real time gli accordi di roaming presenti in quel Paese.
Ciò detto, per un operatore virtuale (assegnatario diretto di risorse di numerazione e che si avvale del proprio operatore di rete ospitante che stipula e gestisce gli accordi con i roaming partner) la fattibilità della soluzione proposta è critica, e non del tutto applicabile, nella misura in cui:
- non dispone di un'informazione sempre aggiornata sullo stato della tecnologia disponibile nei vari Paesi esteri;
- non avendo sotto il suo ambito di responsabilità la stipula e la gestione diretta degli accordi di roaming, non può verificare tempestivamente l'informazione di cui al punto precedente.

B) In riferimento all' Architettura funzionale della soluzione tecnica rappresentata nella slide 10, relativamente all'integrazione degli API fra l'operatore di transito internazionale e l'operatore italiano titolare della numerazione chiamante, si fa presente che:

1) È preferibile implementare una VPN IPSEC fra i due endpoint degli operatori con autenticazione mutua basata su certificati digitali, inoltre sul VPN Concentrator del server che espone a valle le API di implementare un filtraggio IP/porta al fine di consentire il solo raggiungimento dell'interfaccia API che dovrà essere interrogata. Il server Web che espone l'API deve esporre il servizio esclusivamente in HTTPS con almeno TLS1.2 con mutua autenticazione basata su certificati digitali X509. (con questa soluzione VPN IPSERC le reti non avrebbero esposizione su internet - rete IP pubblica.
2) Alternativamente, ove non fosse possibile per policy aziendale implementare la VPN IPSEC tra i due operatori, e si decidesse di esporre direttamente su internet l'interfaccia HTTPS del Web server API, esso deve come protocollo di cifratura ed autenticazione almeno implementare TLS1.2 o superiore, inoltre il WEB Server API esposto su internet non deve essere direttamente raggiungibile da qualsiasi indirizzo IP pubblico, il traffico verso di esso dovrà essere filtrato affinché solamente gli indirizzi IP pubblici autorizzati (operatori che possono chiamare l'API server ossi i carrier internazionali autorizzati in Italia) possano raggiungere il server API sulle sole porte TCP di erogazione del servizio API. La mutua autenticazione sul canale cifrato fra gli operatori dovrà essere basata su certificati digitali X509.

Inoltre sarebbe auspicabile definire un unico standard in termini di formato delle API, parametri, codici di errore, etc. idem per quanto attiene agli eventuali report affinché ci sia lo stesso standard fra tutti gli operatori.
Infine si ritiene possa essere opportuno tracciare e conservare tutte le chiamate agli API Server separatamente da altri servizi per i vari scopi: individuazione di anomalie, reporting, trobleshooting, analisi post mortem incident,….

Restiamo a disposizione per eventuali ulteriori approfondimenti e/o sviluppi

Cordialmente

Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo aggiuntivo al tavolo tecnico

Omissis

Vulnerabilities of telco channels exploited in digital fraud and identified countermeasures

EUROPOL | EC3 European Cybercrime Centre

AG Meeting - October 18th 2022

TLP:AMBER

Fraud Report 2022

CERTFin carries out a survey every year in order to monitor **trends and new patterns of fraud in the banking sector**.

Compared to the previous editions, the 2022 survey was reorganized with the aim of devoting greater attention to the collection of information useful for tracing sets of industry-specific KPIs identified (over 2021) by two working groups focused, respectively, on the field of fraud and cybersecurity.

The 2022 questionnaire consists of 45 questions divided into three main sections:

- **Governance, Scenario and Investments**
- **Fraud**
- **Cyber**

24 banks of different sizes responded with an **overall representation of 87% of the italian sector**, both in terms of customers and employees.

Methodology to investigate the incidence of Telco channels

Starting from the actual frauds, the methods used to finalize the fraud were correlated with the initial vectors (which instead represent the attempted frauds);

Subsequently, the percentage of actual frauds in which the Telco (in the initial and / or final stage) had played a decisive role was calculated.

Once the share (in terms of equivalent value in €) of the actual frauds to be taken into consideration was calculated, **we have the actual fraud amount caused by each initial vector or final step**.

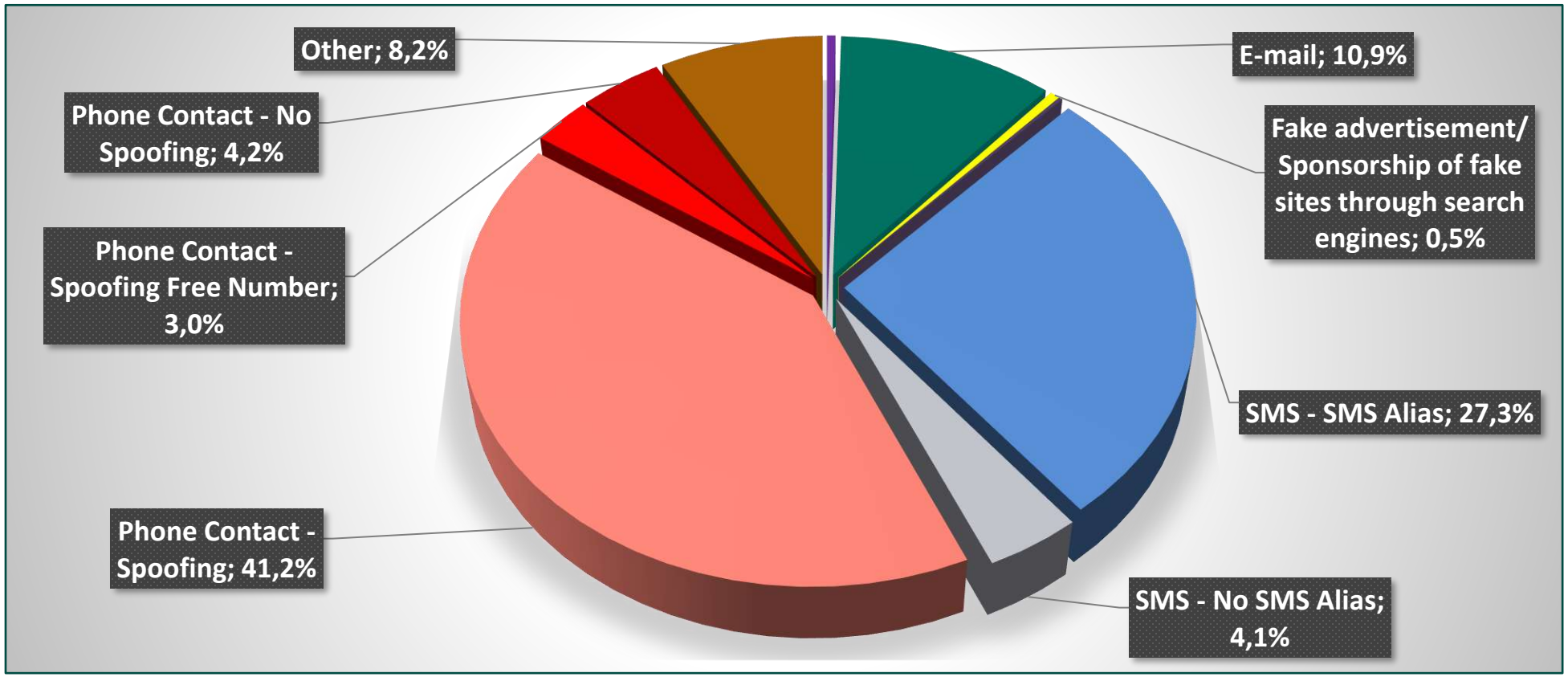
However, a number of estimates and assumptions were made to simplify the calculations: for instance, the average actual fraud was assumed to be constant for each attack technique

Therefore, although reasonable, the following estimates represent only an **approximation of reality.**

Fraud Chain (Retail)

Point of first contact / initial vector of fraud

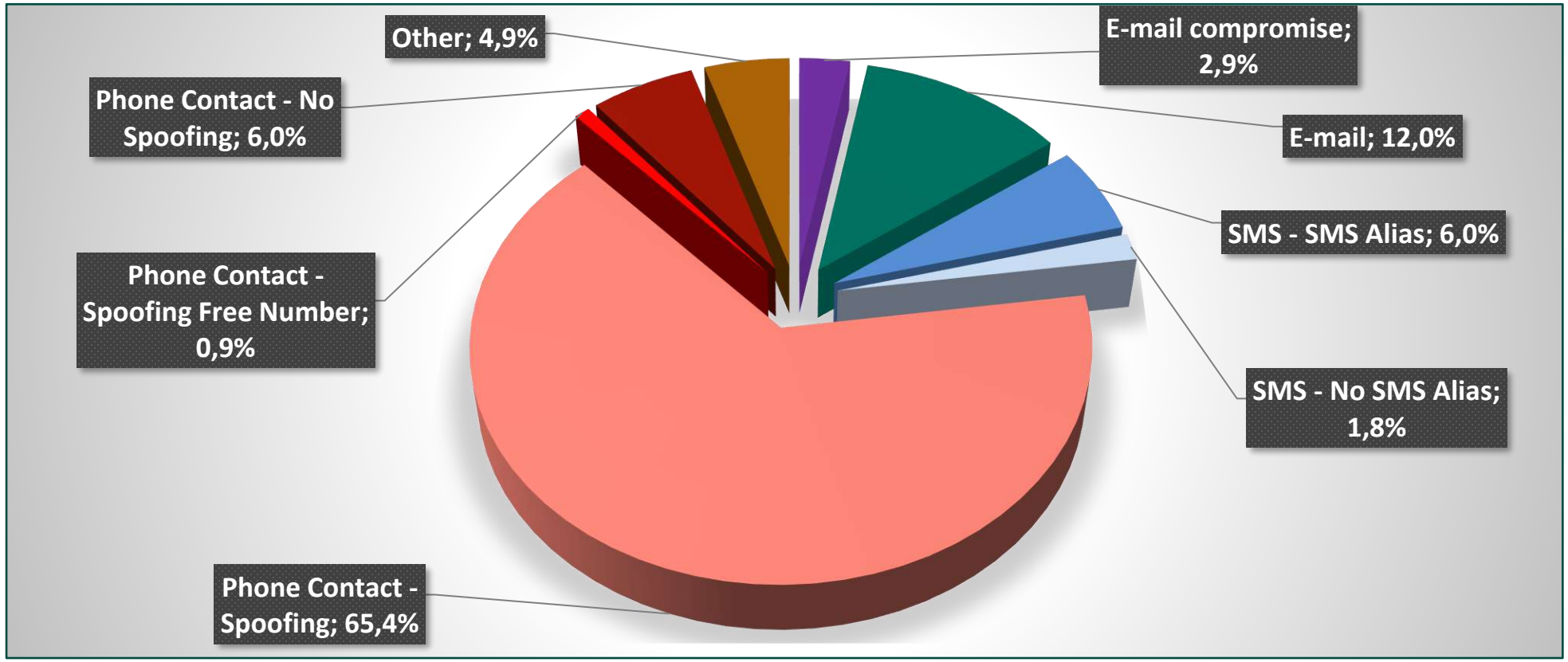
~80% of fraud begins with a phone call or SMS: the fraudsters are increasingly exploiting Spoofing techniques (CLI Spoofing and Alias).



Fraud Chain (Corporate)

Point of first contact / initial vector of fraud

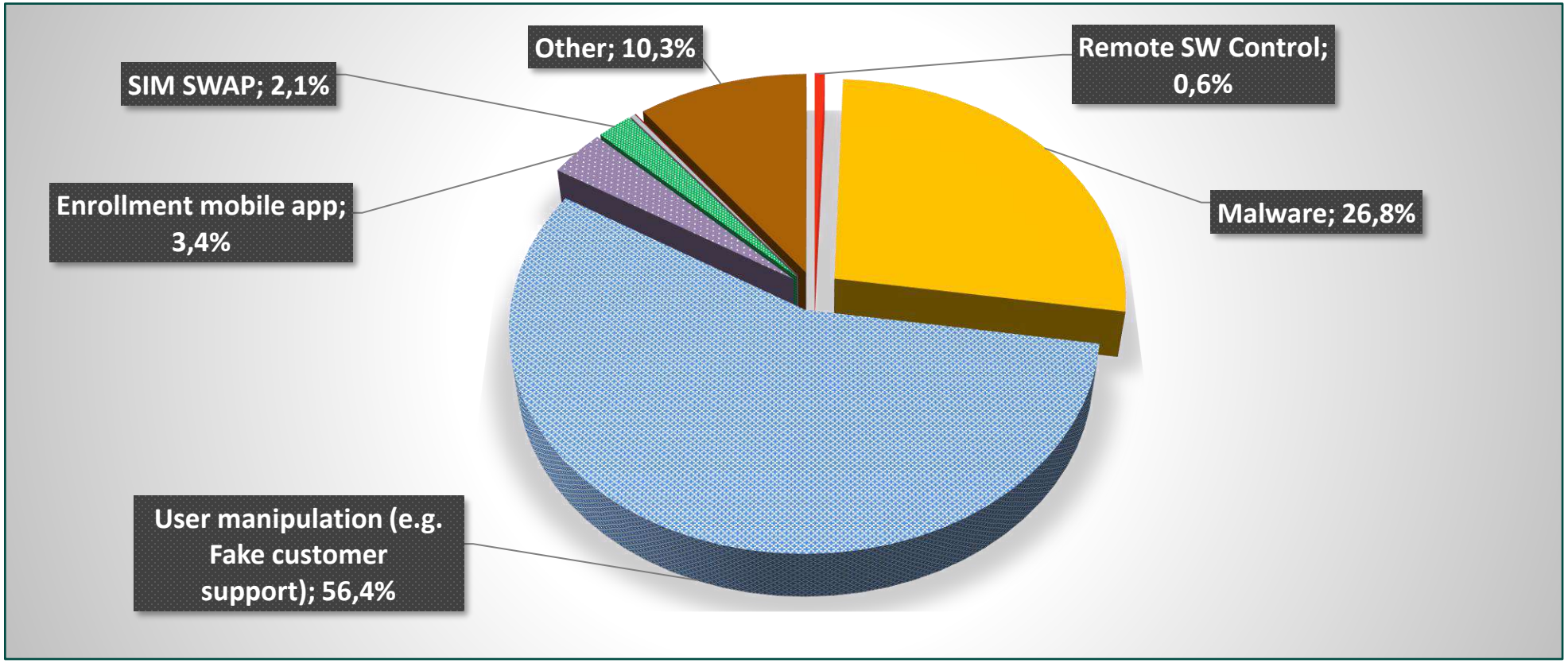
Compared to the Retail segment, there are more cases of fraud carried out by compromising / sending e-mails.



Fraud Chain (Retail)

Technique used to finalize the fraud

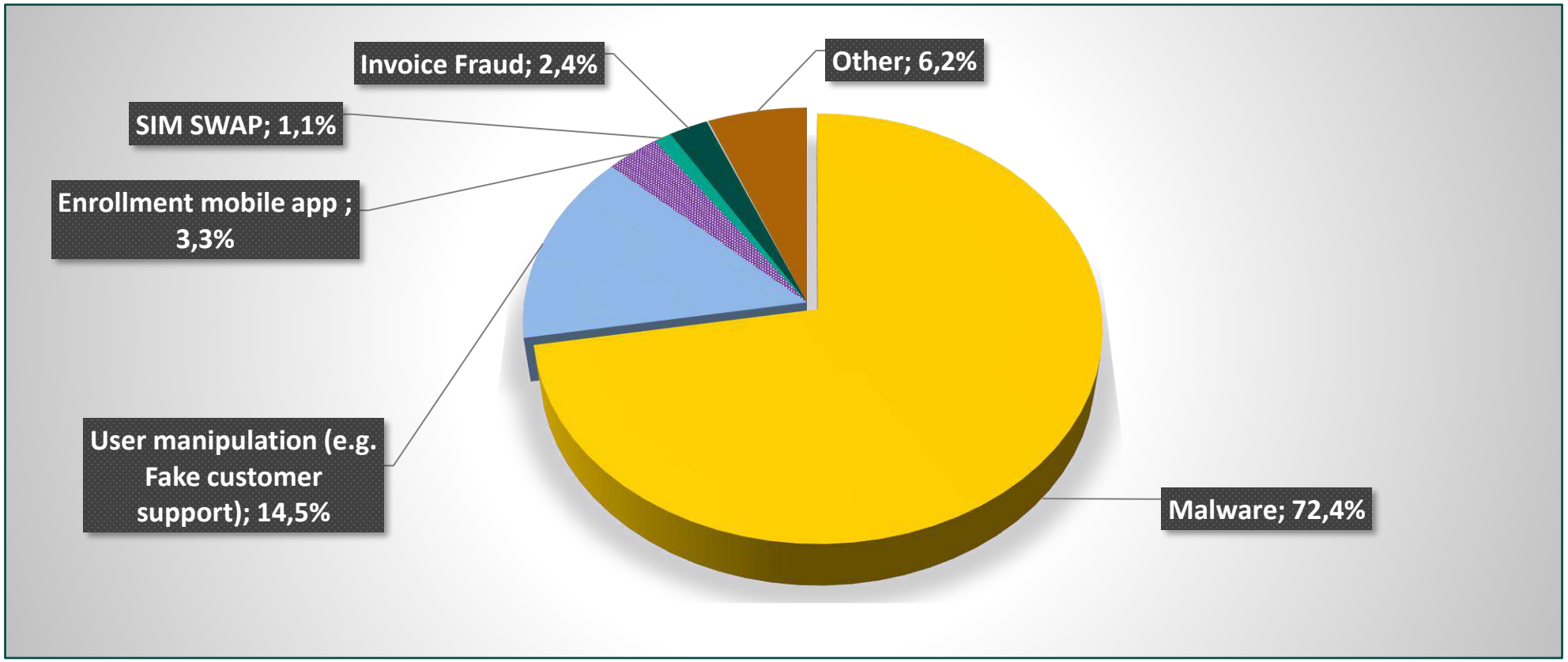
Most fraud is done through user manipulation (56,4%) and malware (26,8%).



Fraud Chain (Corporate)

Technique used to finalize the fraud

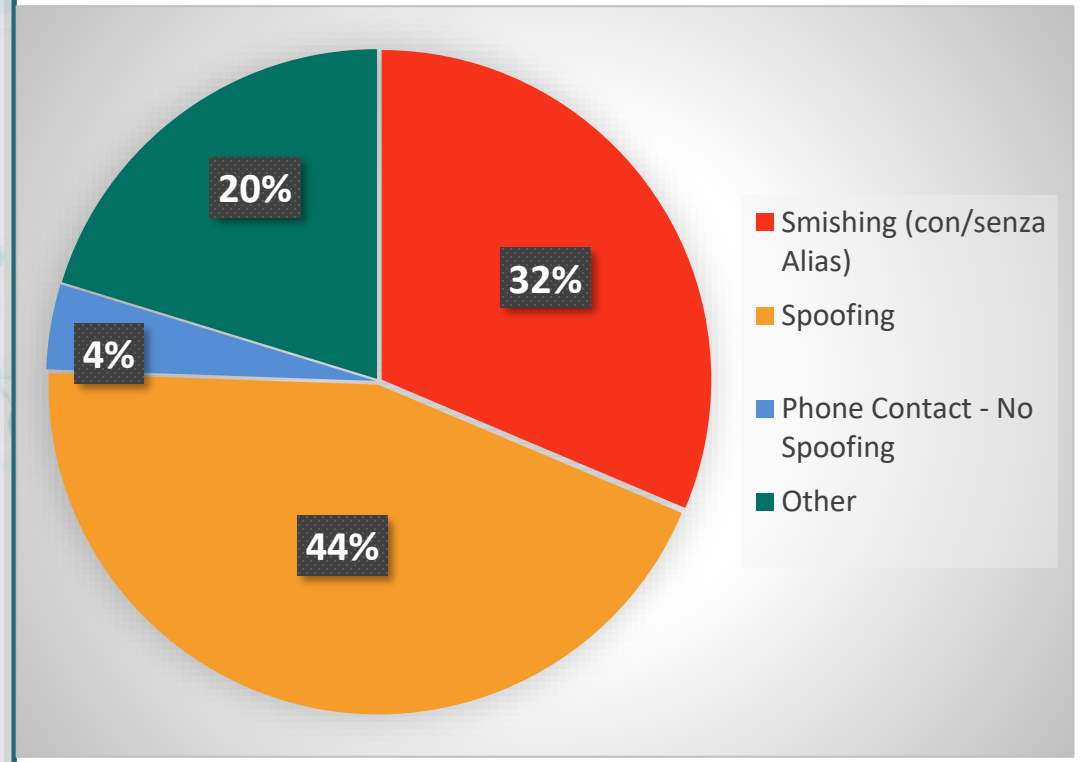
The majority of fraud against Corporate customers is carried out through the use of malware (72,4%).



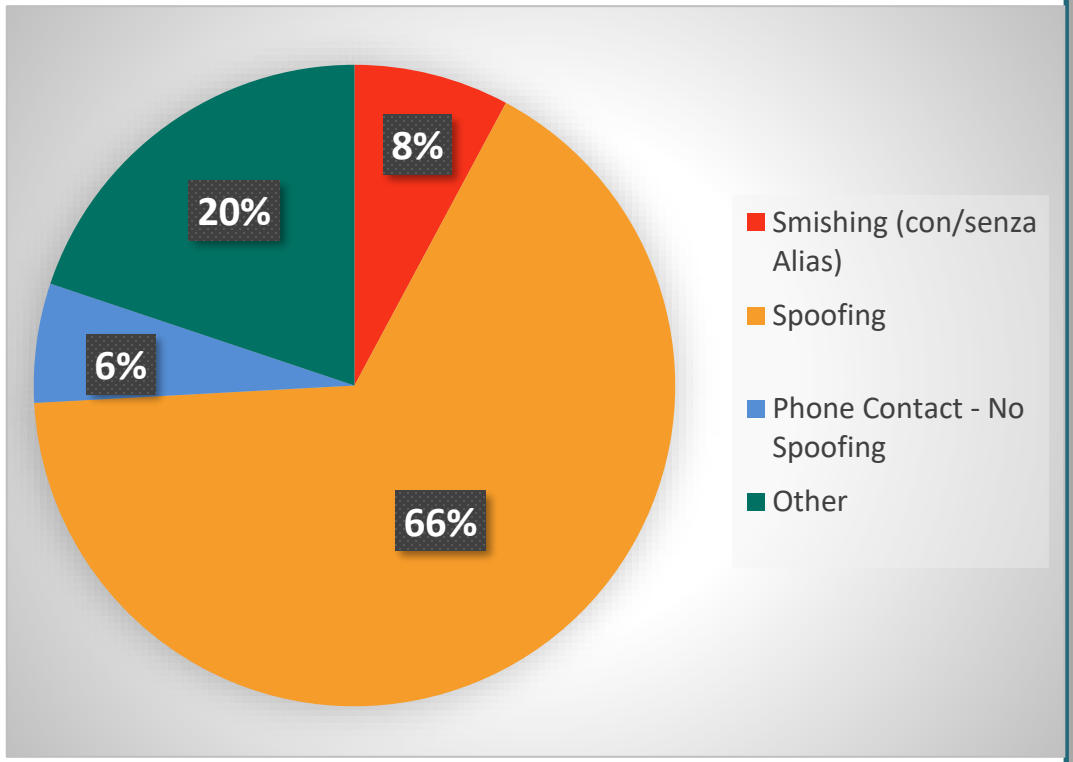
Initial Point of Contact / Initial Fraud vector (Retail & Corporate)

Frauds initiated by **spoofing** have an equivalent value of **€ 13.016.000**; while those implemented through **smishing** (with / without alpha-tag) amount to **€ 9.236.000**.

Retail

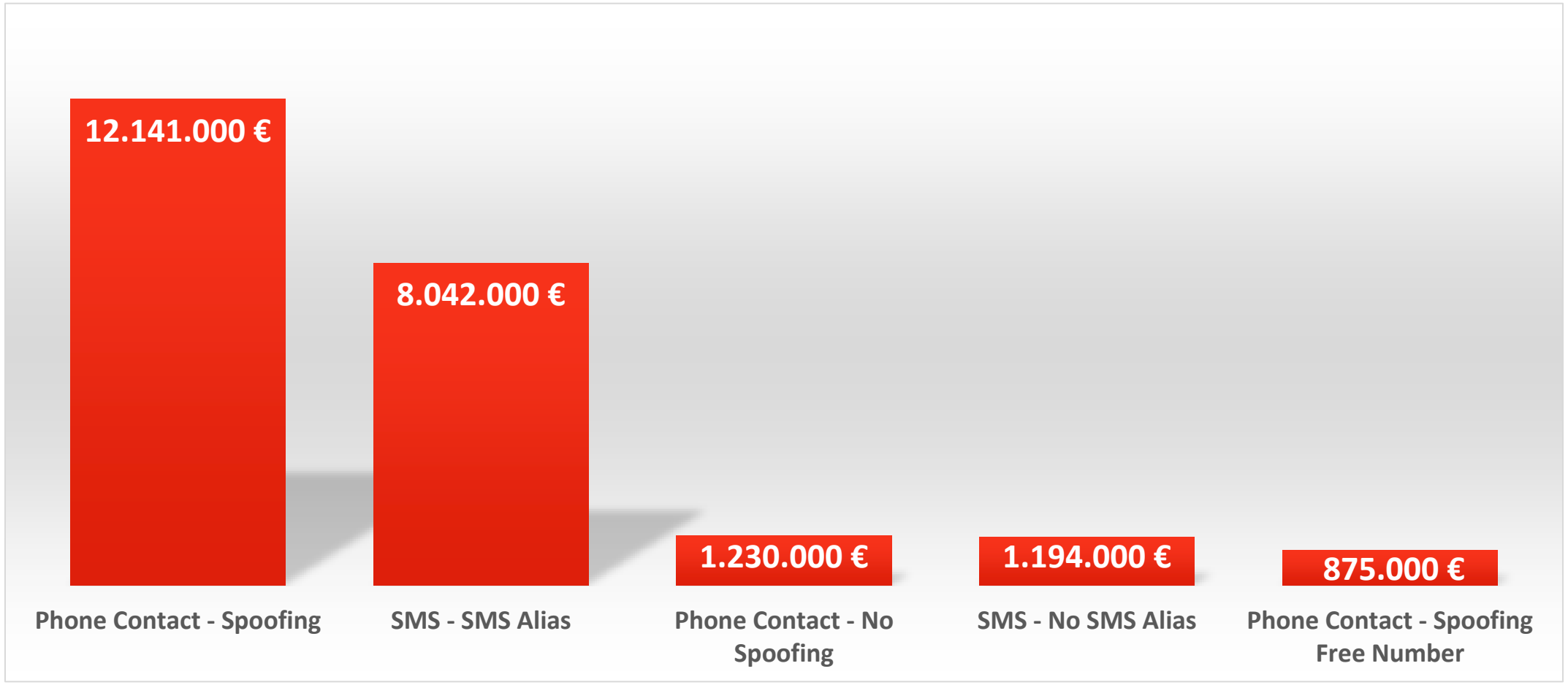


Corporate



Breakdown between contact points / initial vectors of fraud- Analysis on the number of events

Blocked, Recovered and Actual Fraud (Retail segment)



Breakdown between contact points / initial vectors of fraud (Telecommunications Focus)
- Analysis of the value in euro of fraud and number of events (Retail customers)

Blocked, Recovered and Actual Fraud (Corporate segment)

Breakdown between contact points / initial vectors of fraud (Telecommunications Focus)
- Analysis of the value in euro of fraud and number of events (Corporate customers)

Collaboration with AGCOM: Actions undertaken

- **Actions against SIM SWAP**: the path adopted in Italy to combat the SIM SWAP began with the identification of two technical solutions, continued with a trial lasting 18 months and ended with a specific resolution by Italian telecommunications authority (AGCOM). The resolution fully entered into force in several stages, the last of which was completed in September 2022)

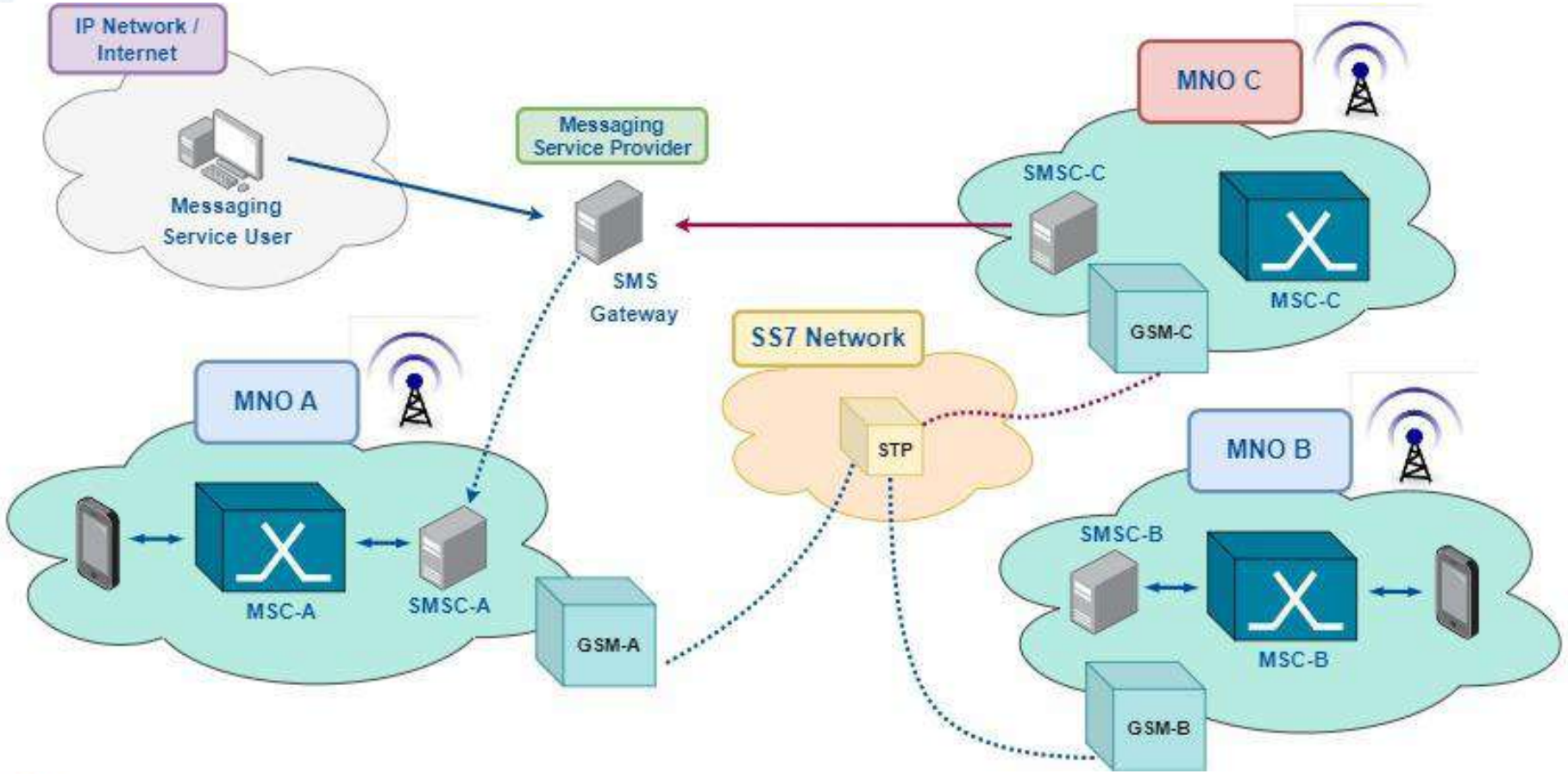
- **Actions against Smishing**: Once collected necessary data, AGCOM resolved the systematic closure / removal of sites / mobile apps linked to services known as "SMS4Cash" through which normal users sold lots of unused text messages to third parties.

- **Actions against Spoofing**: at the beginning of 2022 the ban on delivering calls originating from abroad but which occur at border nodes with the Italian prefix +39 was approved (if they were legitimate they should be generated by Italy, even if roaming)

Alpha-Tag SMS Service
Normal Delivery

1. Request for sending SMS with ALIAS (previously registered in the Alias Register), from a legitimate user (**MSU**) to a messaging provider (**MSP**).
2. The SMS gateway receives messages from national and international entities and requires the SMS to be sent to the **SMSC-A** (short message service center is the portion of a mobile network that handles text message operations) to which it is connected to reach users of the **PLMN-A** (public land mobile network) or, indirectly, users of other PLMN (covered by a different MNO).

...But The SS7 signaling network at **STP** level (A Signal Transfer Point is a node in a SS7 network that routes signaling messages based on their destination point code in the SS7 network) **does not have SMS authentication measures**, therefore various fraud scenarios are possible.

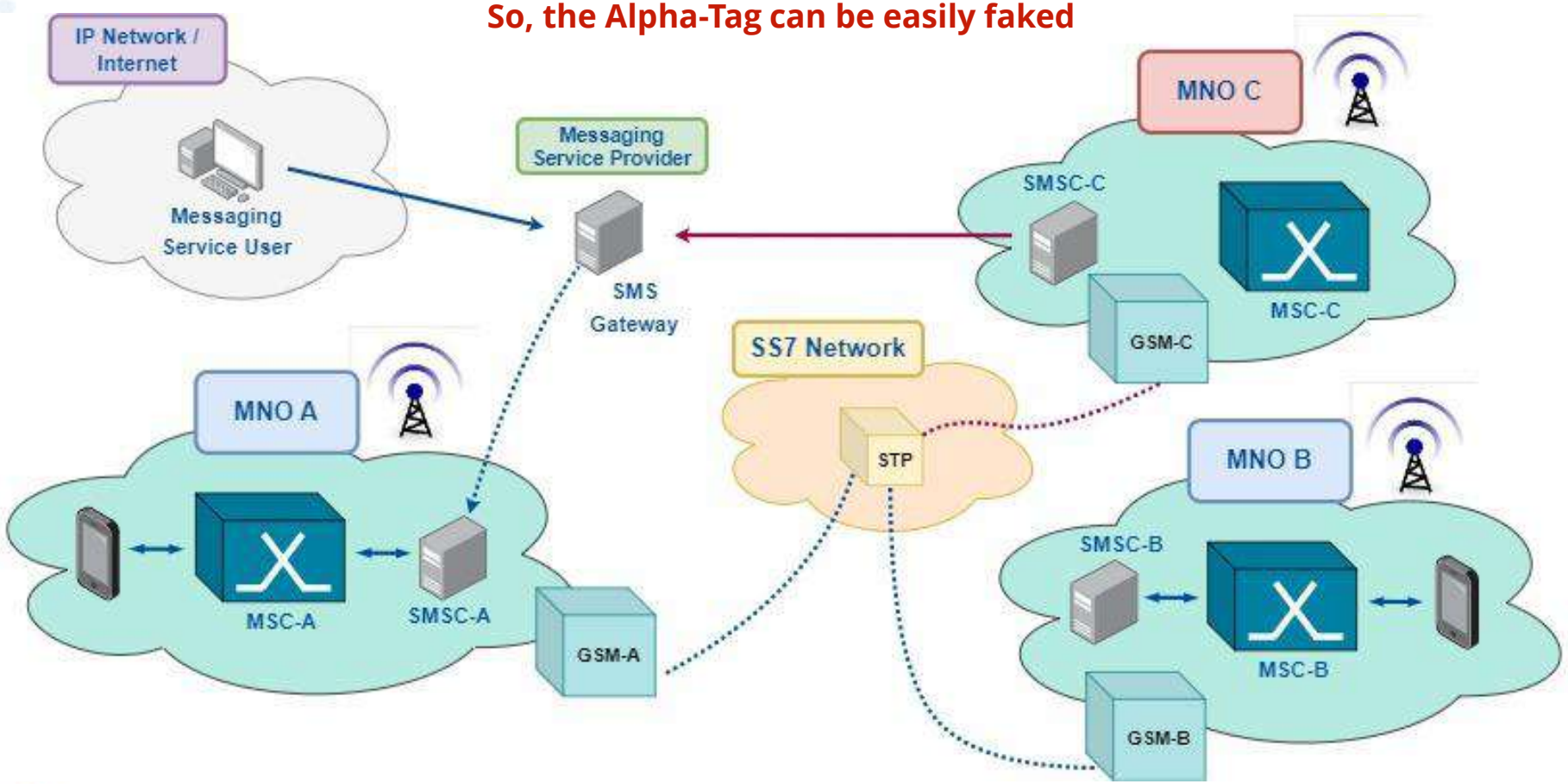


MNO: Mobile Network Operator
MSC: Mobile Switching Centre (core network)

Alpha-Tag SMS Service
Attack Patterns

- The request for sending SMS with ALIAS reaches the SMSC-A from another MNO (MNO C in the figure) with various fraudulent techniques, such as:
  - **SMS Spoofing** (sending via app that simulates the request from an MNO-A user roaming on a foreign operator);
  - **SMS Faking** (e.g. MNO C sends to SMS Gateway an SMS indicating as SMSC-B as sender).
- **Further techniques are possible** (e.g. using web services, other specific devices, etc.) as there is **no control at SMS Gateway level**

So, the Alpha-Tag can be easily faked



MNO: Mobile Network Operator
MSC: Mobile Switching Centre (core network)

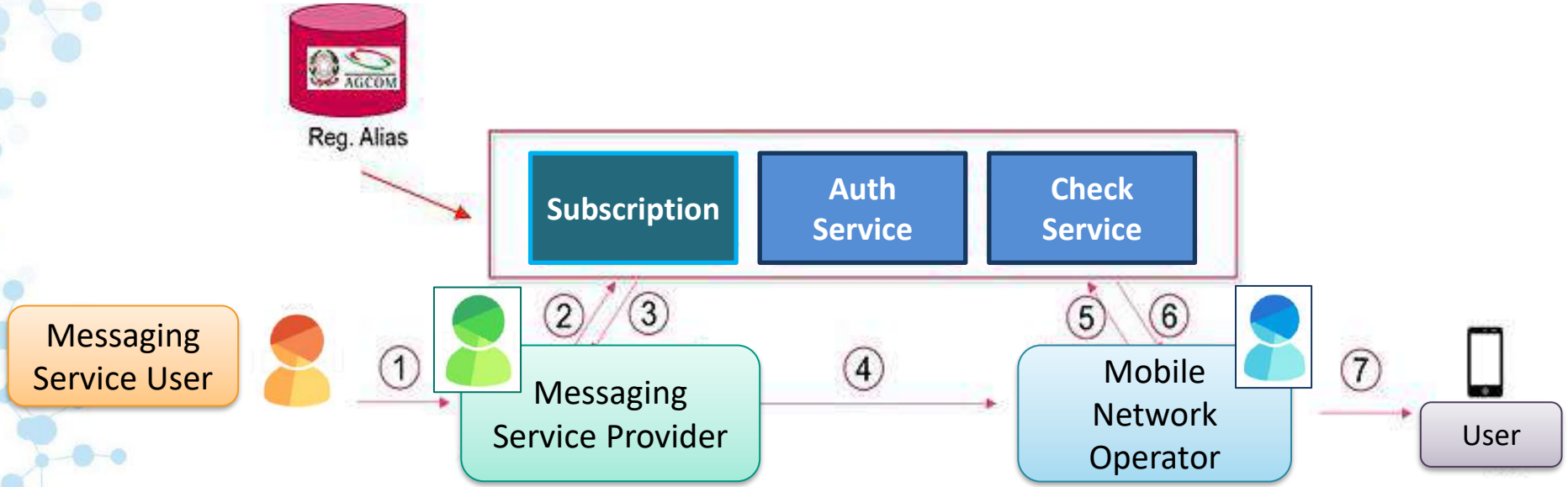
A new technical Solution against fraudulent alpha-tag

- The proposal is based on the creation of an ALIAS SMS Authentication Center (hereinafter referred to as **Authentication DB**) integrated with the AGCOM Alias Register and **uses hashing to certify SMS with ALIAS to be sent.**
- The Authentication DB will be fed from the AGCOM Alias Register, containing the valid Aliases and used for real-time message verification (both Alias and text)
- The Messaging Service Provider (MSP), **before sending each SMS with Alias**, will request certification from the Authentication DB, which will perform the authentication checks, will record a digital fingerprint (hash) of the message and will send a response (accept / reject).
- **The delivery of SMS with Alias will take place with the current network protocol**, which will NOT undergo any changes. The telco operator (MNO), upon receipt of the SMS with Alias from the MSP, before delivering it to the end user, will verify the validity of the SMS, sending a specific verification request to the Authentication DB, which will reply with an appropriate response code (OK / KO), after checking the message.
- Communications with the Authentication DB and the Alias Registry will take place in a secure mode (e.g. Registry services exposed in https and protected by SSL/TLS mutual authentication, i.e. with both Server and Client side certificates and/or a VPN)

14

Authentication process [1/2]

1. Messaging Service User (MSU) requests Messaging Service Provider (MSP) to send messages with ALIAS.
2. For each SMS with Alias, MSP sends the certification request to the Authentication DB providing the following tuple **<ALIAS, MSISDN of the Recipient, Hash = f (Alias, Message text, MSISDN)>**
3. For each certification request received, the Authentication DB:
   - Verify that the ALIAS is valid and the MSP is authorized to use it;
   - **Record the tuple** (ALIAS, MSISDN of the Recipient, Hash of the SMS), assigning it a validity timeout;
   - Send the response code to the certification request.
4. If the certification is accepted, MSP sends the SMS with the ALIAS using the existing protocol.



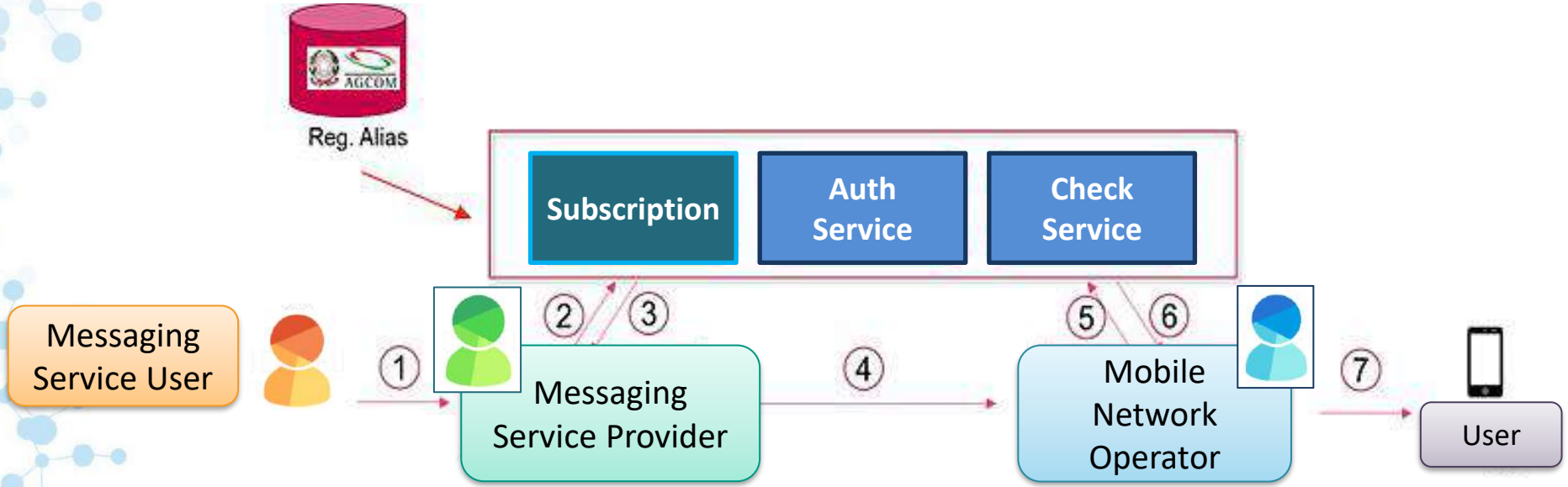
Authentication process [2/2]

5 For each SMS with Alias received, the MNO of the Recipient sends a requests (to the Authentication DB) to verify the message, sending the following tuple:
(Alias, MSISDN of the Recipient, Hash = f (Alias, MSISDN , message text).
Note: The hash of the message is calculated with the same (public) algorithm used by the MSP.

6 For each verification request, the Authentication DB:

- **Verify the existence of the tuple received** from the FSA / FST in the DB;
- Track the outcome of the verification in the DB for analysis and reporting purposes;
- Send the response code (OK / KO).

7 If the verification is successful, MNO delivers the SMS with ALIAS to the end user, **otherwise it blocks the sending of the SMS** and tracks the block in its systems.



Authentication DB
Pros and Cons

Strengths

- Real-time authentication service.
- Ensures authentication of the Alias and message integrity resulting in blocking the delivery of non-certified SMS
- No impact on the SS7 network protocol
- Limited impacts on the operators side for integration with the authentication DB
- Low latency for the execution of the authentication processLong message management (concatenated SMS).
- Scalability of the service with respect to incoming interconnections (international / national)
- Operational continuity of the service

Points of weakness

testing all SMS with Alias could involve a not low cost, especially if we want to also test those originating from Italian networks

A new technical solution for Identity Check

Using information taken directly from the Network Systems and from the services displayed by the operators, through appropriate processing, it is now possible to build some particularly interesting services:

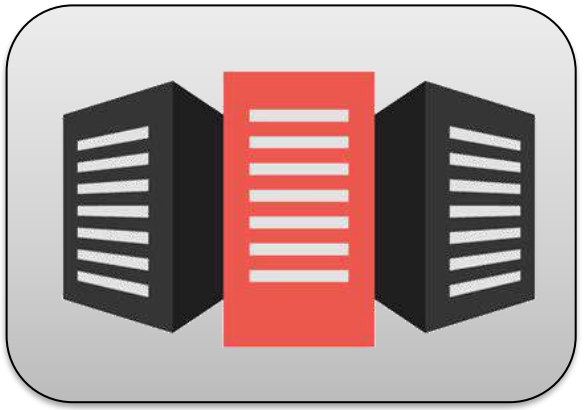
Service	Description
Mobile Operator Ownership	Returns the Mobile Operator to which the mobile number provided in input belongs
SIM SWAP Check	Returns the information if the mobile number provided in input has recently been subjected to the **Mobile Number Portability** procedure (to another operator or new SIM on the same operator)
Mobile Identity Check	Returns the information if the mobile number provided in input is associated with a **specific browsing session** on the data network of an operator
Call-in-progress Check	Returns true if there is a **call in progress on a specific number** (in real time)

Use Case: Mobile Identity
Transaction request from smartphone

1

2

ANTIFRAUD PLATFORM



TIM

WINDTRE

very MOBILE

3

Instant blocking of the operation

1 The hacker has the user's home banking **login credentials**, has installed the app on **his physical device** and requests a bank transfer via mobile phone.

2 The Bank requests the Anti-Fraud Platform to check both the user SIM change and the **navigation IP / telephone number association**

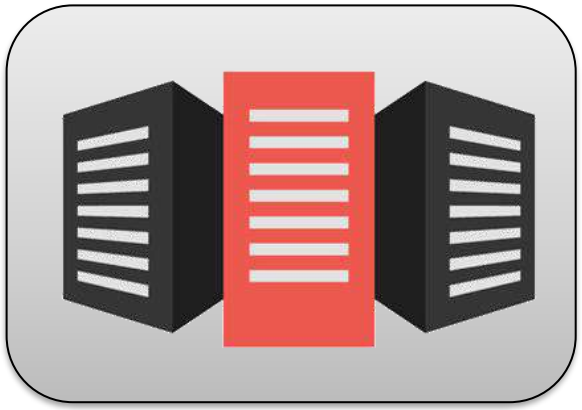
3 The Anti-Fraud Platform returns the information on the SIM change and the **IP-MSISDN association to the bank**. The bank can immediately identify whether the browsing session is actually made by the legitimate user

Use Case: Mobile Identity
Transaction request from PC

1

2

ANTIFRAUD PLATFORM



TIM

WINDTRE

very MOBILE

3

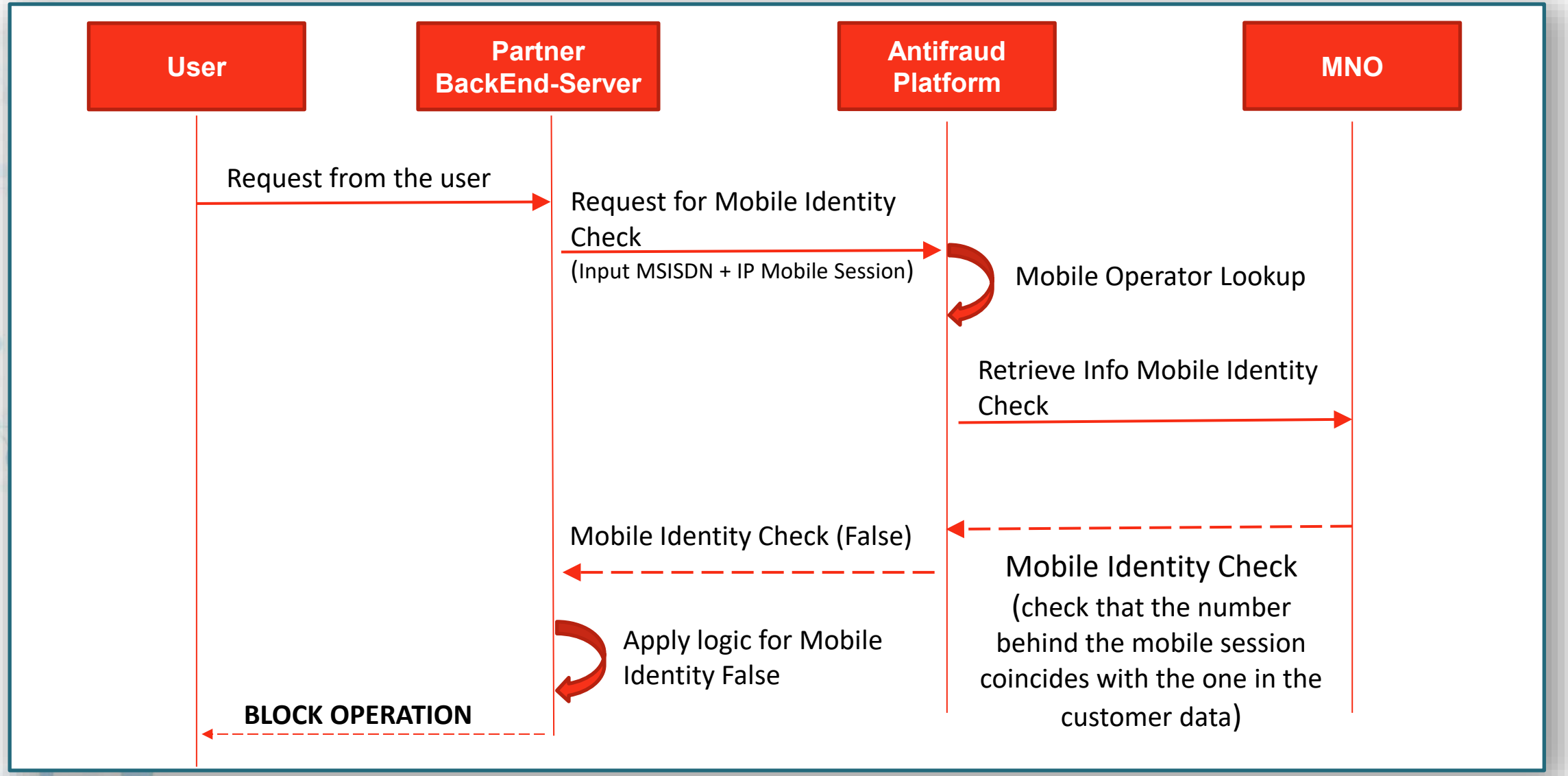
Instant blocking of the operation

1 The hacker has the user's home banking **login credentials**, has installed the app on **his physical device** and requests a bank transfer via personal computer.

2 The Bank requests the Anti-Fraud Platform to check both the user SIM change and the navigation IP / telephone number association **forcing a data session on his mobile device**

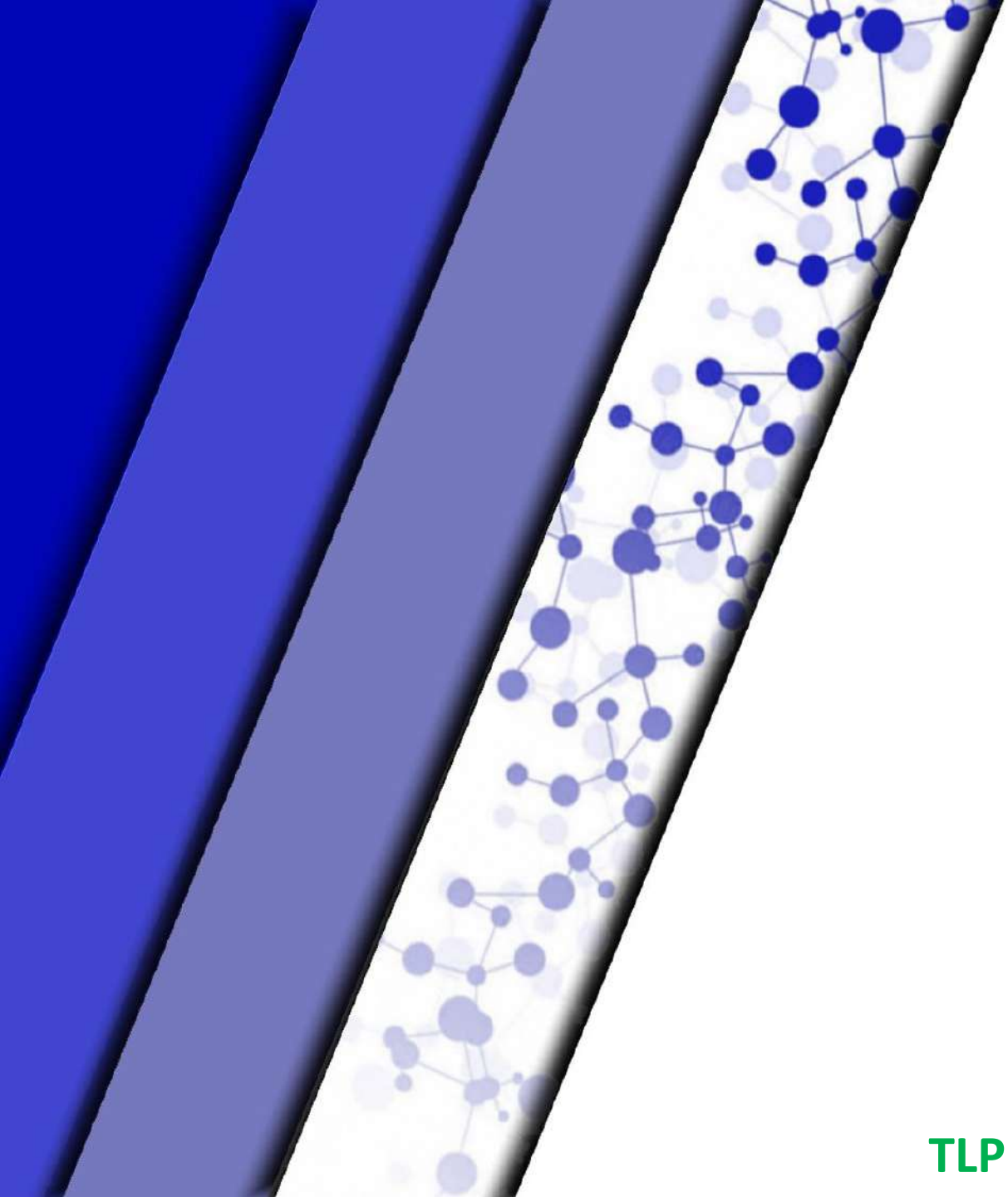
3 The Anti-Fraud Platform returns the information on the SIM change and the **IP-MSISDN association to the bank**. The bank can immediately identify whether the browsing session is actually made by the legitimate user

Logical Scheme: Mobile Identity



Thank You!

Defend. Inform. Evolve.



CLI Spoofing

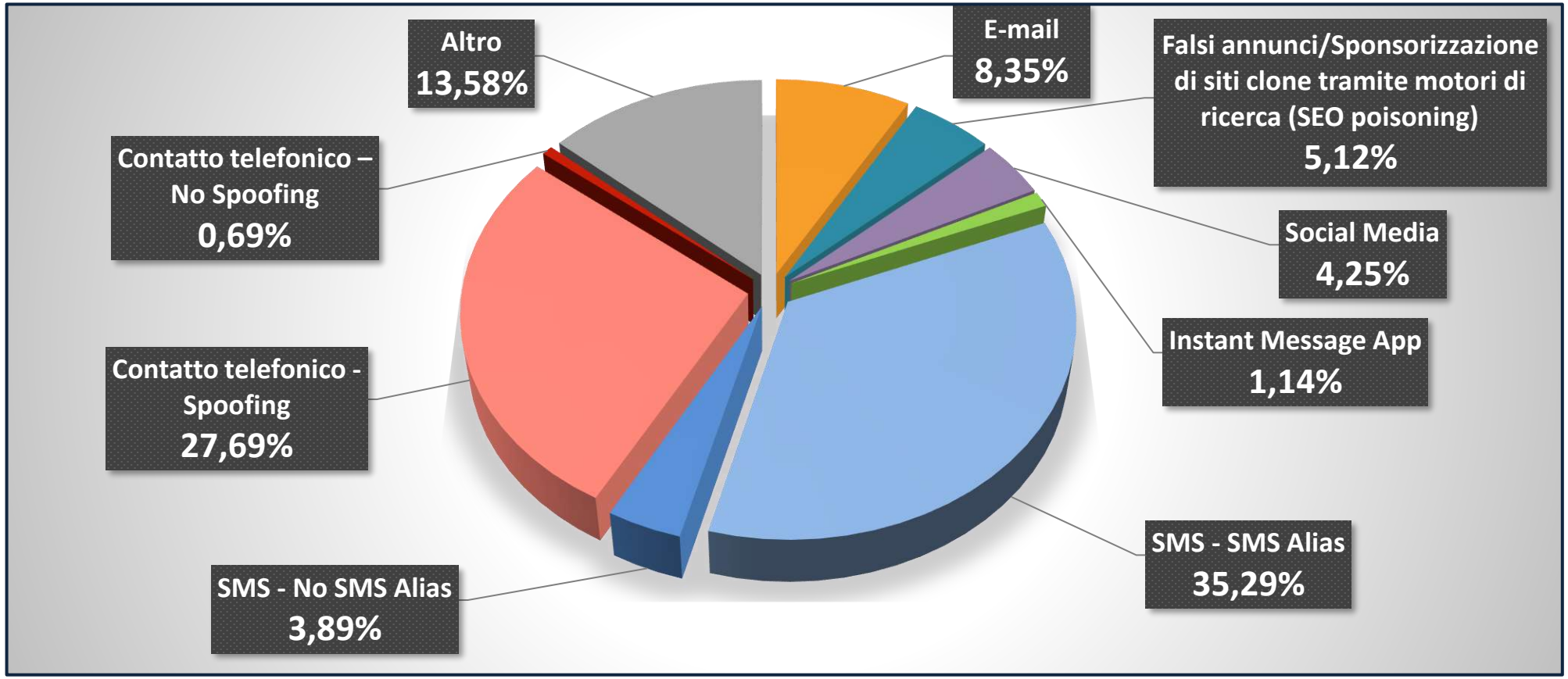
Approfondimenti e considerazioni sulle possibili soluzioni

TLP: GREEN

Fraud Chain

Punto di primo contatto/vettore iniziale della frode

(segmento Retail)

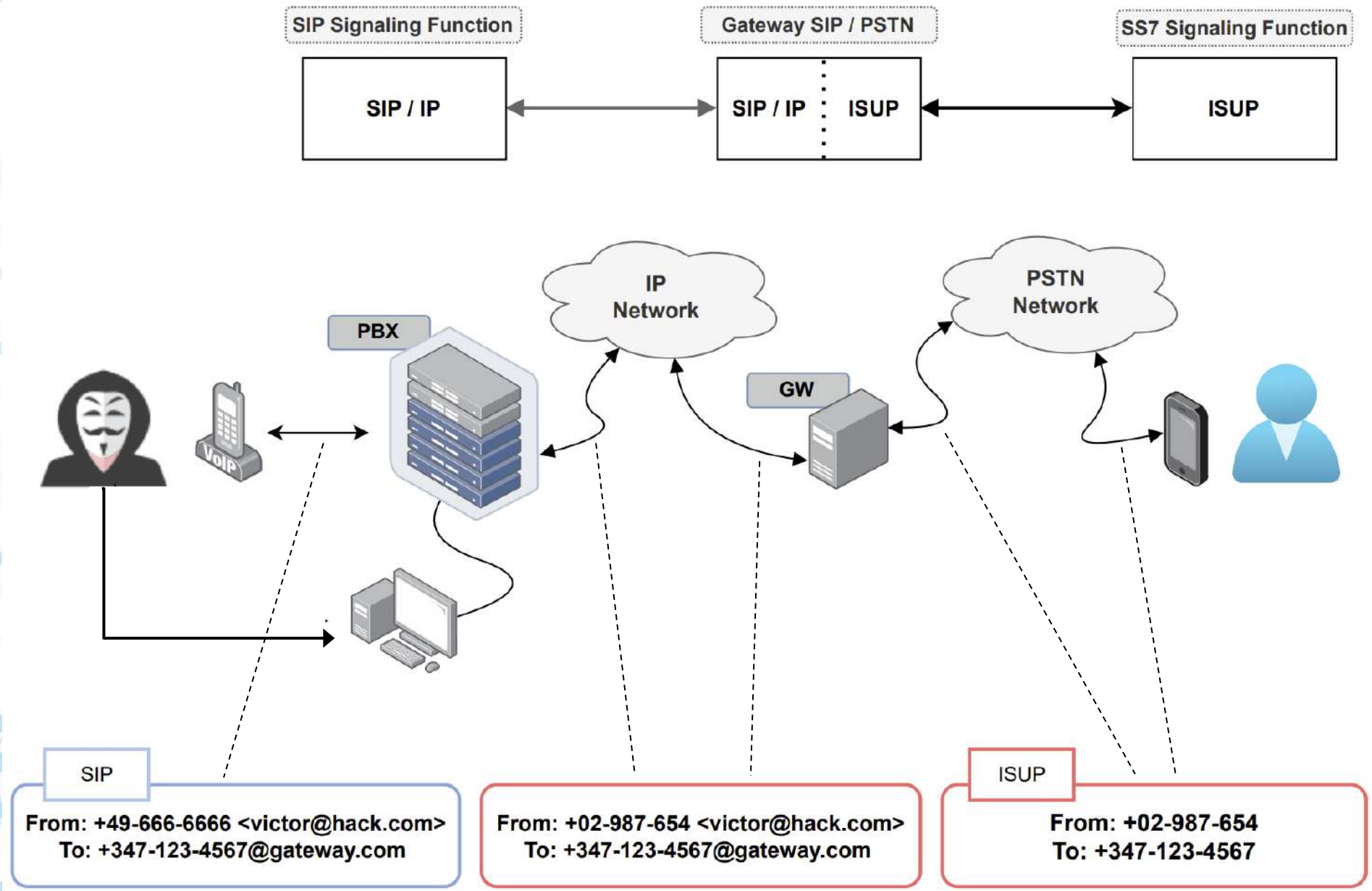


Lo Spoofing è illegale ?

In genere, nella maggior parte delle giurisdizioni, **lo spoofing dell'ID chiamante non è considerato un reato**. Se attraverso lo spoofing si attua un mascheramento che, ad esempio, porta a una frode, allora si configura un reato. Ma il reato è la frode, non lo spoofing!

Ci sono casi in cui lo spoofing è legittimo: un medico che chiama dal suo cellulare ma l'ID che appare sul dispositivo del paziente è quello dell'ospedale, oppure meccanismi aziendali utili a proteggere la privacy dei dipendenti che lavorano nel call center.

Come avviene lo Spoofing



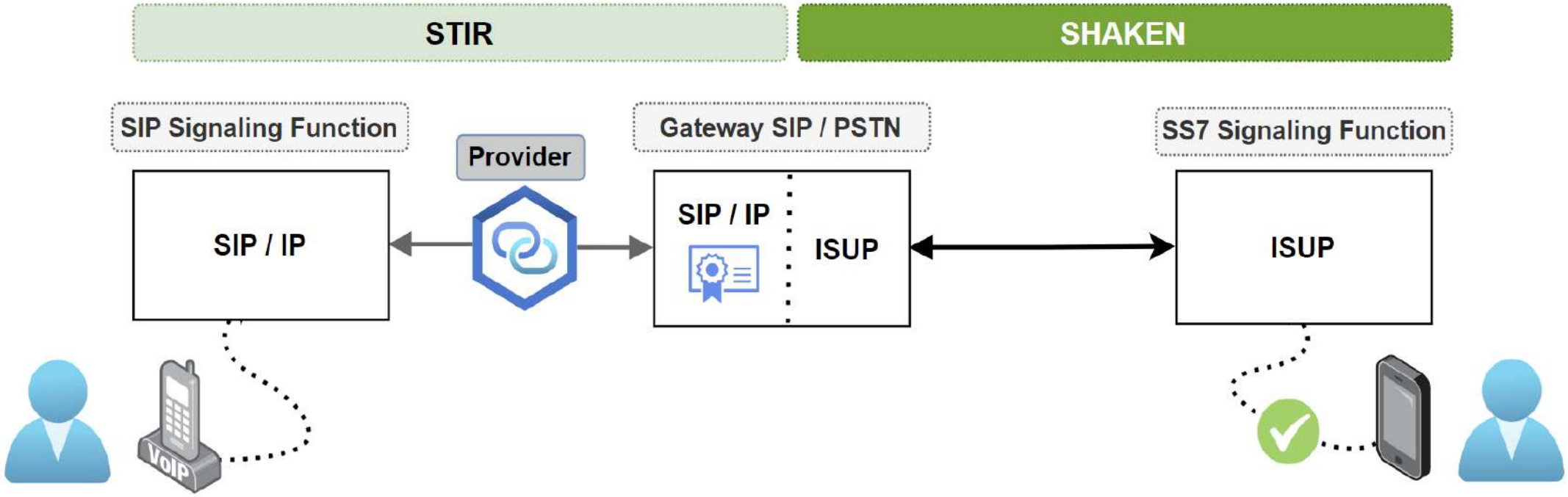
STIR & SHAKEN

STIR/SHAKEN è una suite di protocolli e procedure per combattere il CLI spoofing sulle reti telefoniche pubbliche.

STIR, acronimo di **Secure Telephony Identity Revisited**, è stato definito in una serie di documenti standard RFC da un gruppo di lavoro della Internet Engineering Task Force. **Funziona aggiungendo semplicemente un certificato digitale alle informazioni del Session Initiation Protocol** (SIP) utilizzate per avviare e instradare le chiamate nei sistemi VoIP.

SHAKEN, acronimo di **Signature-based Handling of Asserted information using toKENs.** è invece una serie di linee guida per le reti telefoniche pubbliche commutate le quali indicano come gestire le chiamate con informazioni STIR errate o mancanti.

STIR / SHAKEN

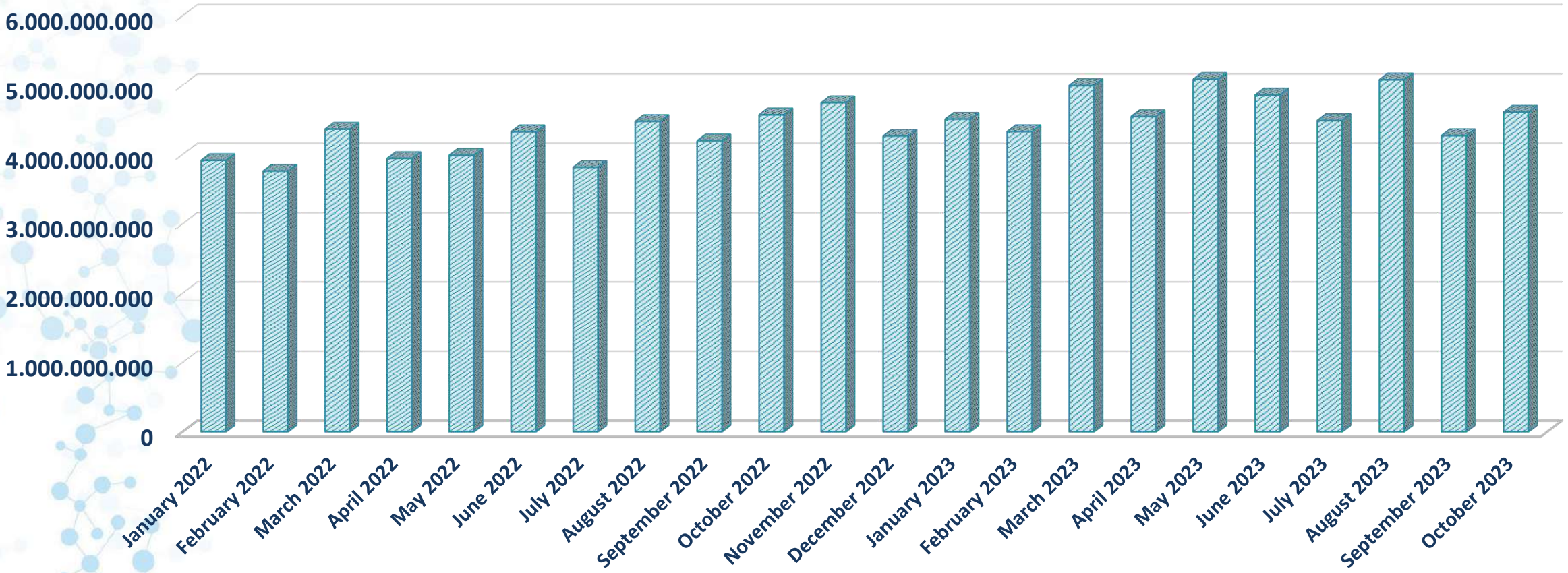

STIR
SHAKEN
SIP Signaling Function
Provider
Gateway SIP / PSTN
SS7 Signaling Function
SIP / IP
SIP / IP
ISUP
ISUP
VoIP

STIR / SHAKEN

- STIR/SHAKEN è, dunque, una suite di protocolli in grado di «autenticare» le chiamate e contrastare lo spoofing
- Negli USA norme prescrittive dettate dal **Traced Act**, entrate in vigore progressivamente dal 2020, hanno imposto STIR/SHAKEN alle aziende di telecomunicazioni statunitensi
- Gli operatori statunitensi hanno speso collettivamente oltre **mezzo miliardo di dollari** nell'implementazione
- Emerge la chiara intenzione di imporre progressivamente le stesse modalità di verifica alle chiamate internazionali

Attuale Situazione in US

Number of US Robocalls since STIR/SHAKEN became mandatory



Source: YouMail Robocall Index [*https://robocallindex.com*]

Anti-Spoofing measures around the world (1/4)

🇺🇸 🇨🇦 **US** e **Canada** hanno adottato STIR/SHAKEN

🇦🇺 **Australia**: Blocco delle chiamate internazionali non in roaming in entrata che hanno un CLI che sembra di origine nazionale.

- Attualmente si concentra sul blocco delle chiamate che utilizzano numeri di rete fissa australiani, ma si sta cercando di estendere anche ai numeri di rete mobile.
- Whitelisting di parte del traffico proveniente da call center con sede all'estero.
- Codice di condotta promosso da *Communications Alliance LTD*
- Riduzione del 50% delle chiamate truffa segnalate dai consumatori da quando è stato introdotto il Codice
- È facile capire perché altri Paesi e telco potrebbero adottare questo approccio.

Anti-Spoofing measures around the world (2/4)

 **China**: La Cina imporrà uno «**smell test**» ai vettori che gestiscono il traffico internazionale. Ciò significa che può decidere di bloccare i vettori che non soddisfano i requisiti, talvolta arbitrari, di come dovrebbe essere un buon traffico. Significa anche che possono trovare motivi per favorire le telco che preferiscono e punire le telco (i Paesi) che non amano.

 **Finland**: La soluzione si basa su un lavoro di validazione affidato agli stessi operatori: l'operatore nazionale su cui arriva una chiamata internazionale **è incaricato di verificare l'affidabilità del vettore**, successivamente firma la chiamata. Tutti gli operatori su cui la chiamata transita prima della terminazione sanno che la chiamata è stata verificata.

Anti-Spoofing measures around the world (3/4)

🇬🇧 **UK**: Il Regno Unito ha formalizzato la sua versione del blocco delle chiamate internazionali in entrata con un CLI nazionale nello standard **NICC ND 1447**.

Dall'introduzione di questa misura si è registrata una riduzione del 65% dei reclami per chiamate truffa. (source: TalkTalk.co.uk)

🇩🇪 **Germany**: Non bloccare le chiamate (con alcune eccezioni), ma invece eliminare il CLI delle chiamate internazionali non in roaming in entrata che hanno un CLI che sembra nazionale.

🇫🇷 **France**: L'Autorità francese ha reso obbligatorio il blocco delle chiamate se il CLI non è autenticato, ma non ha prescritto come autenticare le chiamate. Pertanto, l'Associazione Telco Francese (APNF) si avvia a definire **una versione francese di STIR/SHAKEN**.

Anti-Spoofing measures around the world (4/4)

 **Belgio**: È in attuazione un metodo basato su una **DNO List**: la compilazione di un elenco nazionale di numeri di telefono "Do Not Originate" (DNO) (mantenuto a livello centrale) in grado di ridurre le chiamate truffa in cui il numero di telefono viene spoofato per farlo corrispondere a un numero presente nella lista (es. associato a un dipartimento governativo o ad un numero di contatto di una banca).

 **Italia**: Al momento l'AGCOM ha circolato solo raccomandazioni di blocco nel caso di chiamate *inbound* non conformi alla specifica E.164 (Country Code assente o non conforme) o di chiamate internazionali non in roaming ma con CLI domestico.

 **UE**: Il BEREC, l'agenzia dell'UE per la regolamentazione delle comunicazioni, non ha ancora indicato come intende combattere lo spoofing a livello europeo.

Rich Call Data

Rich Call Data (RCD): tecnologia rivolta alle grandi aziende che consente di inviare informazioni sul chiamante ai destinatari, visibili prima che questi rispondano (es. il nome dell'azienda, il logo e persino il motivo della chiamata). La telco di origine allega i dati, la telco di terminazione organizza il modo in cui questi dati vengono presentati.

- *Può essere fornito da soluzioni fuori banda come Verified Calls di Google.*
- *Potrebbe essere realizzata come add-on alle firme SHAKEN; avrebbe gli stessi svantaggi di STIR/SHAKEN o potrebbe essere una firma RCD*
- *Elevati standard KYC per le firme RCD saranno fondamentali per il successo di questa offerta.*

Out of Band Approach

Perché non utilizzare un metodo ***fuori banda*** per verificare la legittimità delle chiamate?

- Comunicazione su un canale diverso per chiedere se il CLI rappresenta la vera origine della chiamata.
- La telco di origine scrive i dati della chiamata su un server; la telco ricevente li consulta.
- Le telco potrebbero scrivere e leggere i dati su un server condiviso.
- Più economico e veloce da implementare rispetto ai metodi *in banda*

La Communications Business Automation Network (CBAN) ha in corso una sperimentazione su questo metodo.

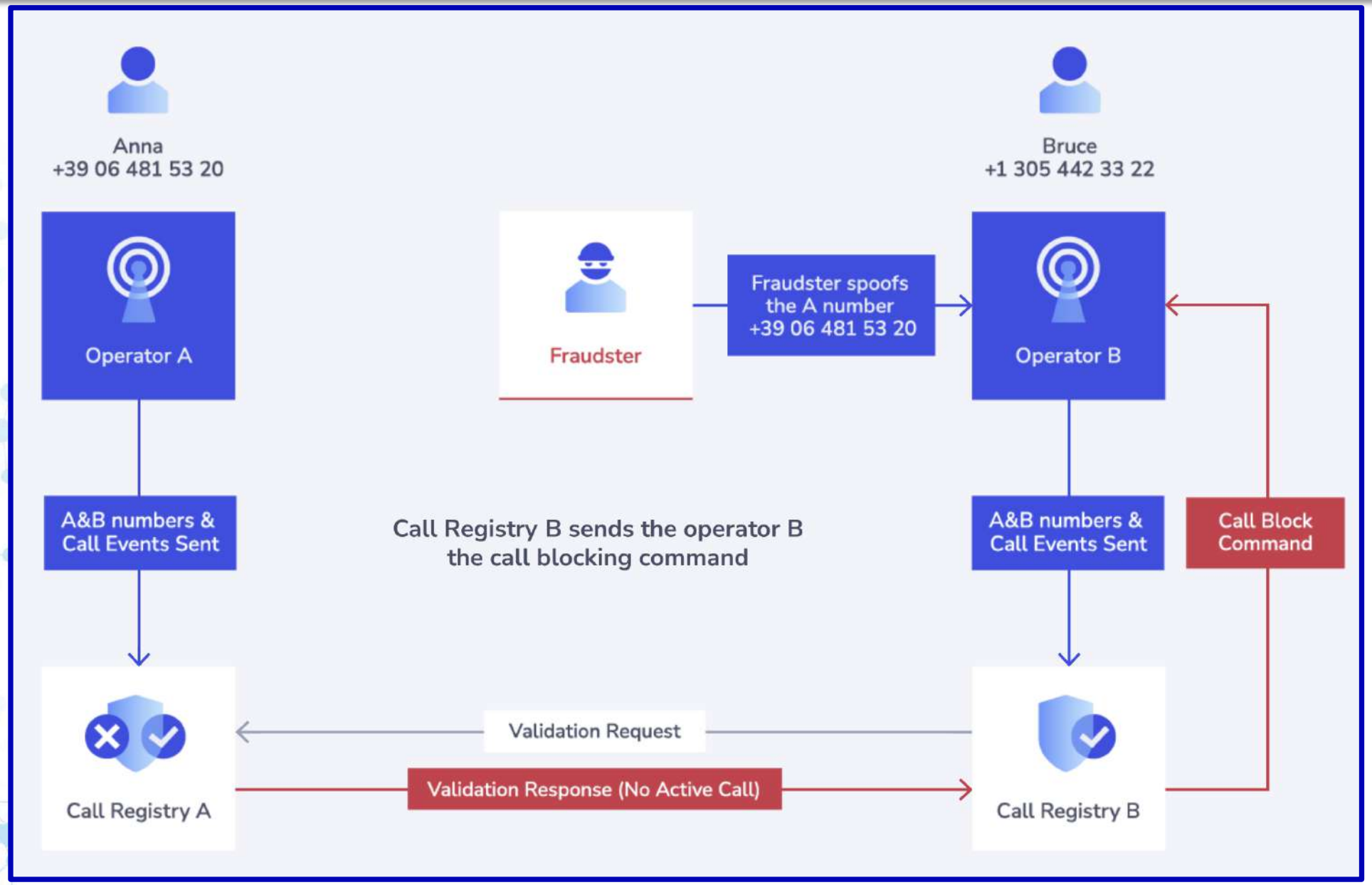
AB Handshake

Funziona creando un "**handshake**" **fuori banda** tra la telco che origina la chiamata e quella che la termina. L'AB Handshake garantisce che qualsiasi chiamata vocale sia convalidata sia dall'operatore di origine che da quello di terminazione, rendendo impossibile commettere frodi basate sulla manipolazione del traffico da parte di intermediari.

Processato parallelamente all'impostazione della chiamata, l'"handshake" fornisce a entrambe le parti A e B la conferma che i parametri della chiamata sono coerenti, altrimenti offre la possibilità di interrompere le chiamate non valide.

AB handshake funziona potenzialmente per tutti i tipi di chiamate tra tutti i tipi di reti in tutti i Paesi.

AB Handshake



Problema tecnico o politico?

- Negli Stati Uniti il dibattito si è concluso prima di iniziare, perché l'uso di STIR/SHAKEN per contrastare il CLI spoofing è già incorporato nella legge statunitense.
- Tutte le reti IP negli Stati Uniti dovranno utilizzare STIR/SHAKEN; L'errore principale è stato quello di **prescrivere una tecnologia** prima che si sapesse quanto fosse efficace.
- Di conseguenza, molti dibattiti che nominalmente riguardano le modalità di implementazione di STIR/SHAKEN in realtà non riguardano affatto la tecnologia, perché la decisione principale è stata quella di utilizzare la PKI.
- **International SHAKEN** è il tentativo di far quadrare il seguente cerchio:
  - *Gli Stati Uniti vogliono sapere di quali chiamate estere ci si può fidare.*
  - *Altri Paesi che adottano un metodo basato su PKI vogliono sapere lo stesso.*
  - *Alcune società di telecomunicazioni dovranno conformarsi a più regimi di governance indipendenti di diversi Paesi o ci sarà una condivisione della sovranità sulle firme?*

Problema tecnico o politico?

Se la firma non viene applicata dalla telco di origine, i vantaggi della firma sono dubbi: negli Stati Uniti **le chiamate firmate affette da spoofing sono 5-6 volte superiori a quelle non firmate**.

Altri paesi si stanno scervellando per decidere se implementare la stessa tecnologia, ma **la questione fondamentale riguarda la governance**: se tutti i Paesi del mondo utilizzassero la stessa tecnologia ma avessero modelli di governance diversi, **una firma applicata in un Paese non avrebbe alcun valore in nessun altro Paese**.

È chiaro che c'è anche un problema di scalabilità: Stati Uniti e Canada hanno concordato di implementare STIR/SHAKEN in tandem e hanno implementato una tecnologia equivalente in ciascun Paese, ma non hanno ancora trovato un quadro di governance comune che si applichi alle chiamate che passano tra i due Paesi.

International SHAKEN

- Necessità di creare un «club» di regolatori nazionali che possano concordare tra loro la sua adozione
- I principali sostenitori di *International SHAKEN* ne promuovono l'adozione attraverso i **certificati delegati**: il lavoro di un'autorità di certificazione in un paese è attendibile anche presso l'architettura di governance di un altro paese.
- Sembra una soluzione ovvia, ma il problema di fondo è che le autorità di regolamentazione faticano a stabilire di quali telco ci si possa fidare e quali invece debbano essere ritenute inaffidabili.
- Il KYC è fondamentale per evitare che l'infrastruttura di autenticazione venga sovvertita: gli Stati Uniti hanno già dimostrato un'incredibile ingenuità nei controlli KYC, con il risultato che le chiamate firmate hanno più probabilità di essere spoofate rispetto a quelle non firmate
- Inoltre, è necessario verificare che tutte le autorità di certificazione siano in grado di completare il processo entro i 500 ms, al fine di evitare potenziali problemi tecnici.

International SHAKEN: Come potrebbe funzionare

- È necessario applicare solidi standard KYC ad ogni anello della catena di delega per garantire che i certificati siano utilizzati solo per firmare chiamate attendibili ...Ma nessuna Autorità può far rispettare le proprie regole al di fuori del proprio Paese.
- Certificati delegati in mano ad operatori di frontiera consentirà a questi soggetti di firmare le proprie chiamate
- Queste debolezze sono fondamentali per capire perché negli Stati Uniti vengono firmate chiamate «malevole».
- Se questo è ciò che accade all'interno di un ecosistema in cui l'autorità nazionale ha poteri illimitati, è facile capire come le cose possano andare molto peggio quando più autorità di governance devono dividere/condividere/delegare le responsabilità.
- ATIS (Alliance for Telecommunications Industry Solutions) sta esplorando un'alternativa ai certificati delegati promuovendo una soluzione basata su DLT.

Conclusioni

- Necessità chiara e crescente di affrontare il problema del CLI spoofing della CLI sia in ambito *consumer* che *wholesale*
- Alcuni metodi richiedono un certo grado di **cooperazione** (potrebbero essere imposti alle società di telecomunicazione se non agiscono su base volontaria)
- La linea di demarcazione principale è tra i metodi ***in banda*** e quelli ***fuori banda***
- **STIR/SHAKEN** è il metodo più conosciuto e testato perché gli US hanno legiferato per primi.
- Le firme digitali funzionano solo se supportate dai carrier, ma al momento non sono utilizzate in modo tale da affrontare le frodi di cui i carrier sono vittime.
- I metodi *out of band* utili a proteggere i consumatori necessitano solo del supporto delle telco all'inizio e alla fine della chiamata, ma potrebbero essere adottati anche per contrastare le frodi all'ingrosso. **Accordi bilaterali** potrebbero favorirne la diffusione.
- Difficile immaginare un uso transfrontaliero delle firme digitali a causa di difficoltà nella gestione degli aspetti di **governance**.

Proposta

Misura di base

Rendere obbligatorio il blocco delle chiamate internazionali non in roaming in entrata che hanno un CLI che sembra di origine nazionale (con alcune eccezioni ben definite che saranno gestite da un meccanismo di whitelisting)

[*verifica piuttosto semplice per un MNO attraverso un HLR lookup*]

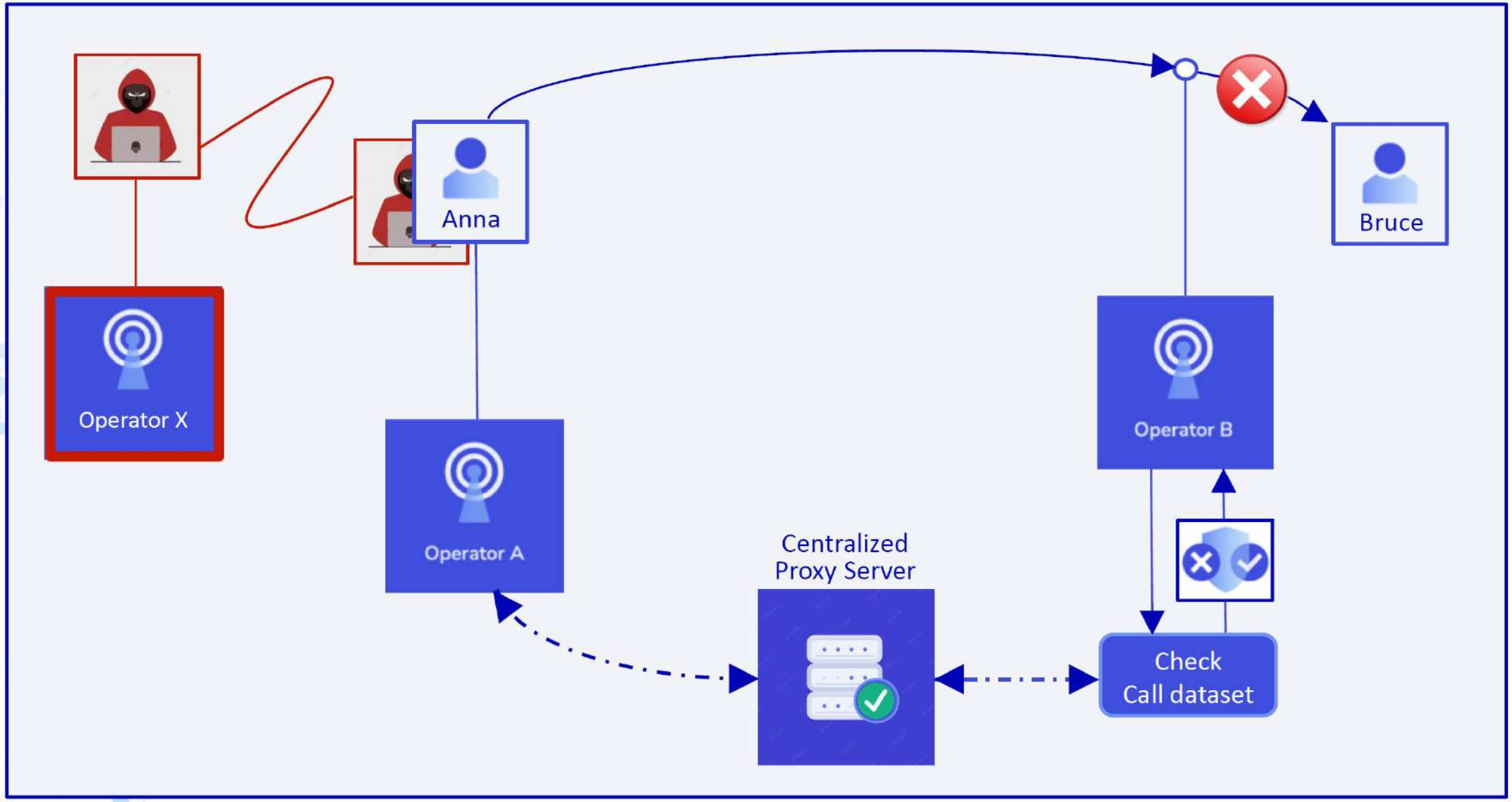
Soluzione ottimale

Convalida fuori banda: realizzazione di un ***proxy server***, gestito da un soggetto trusted, che intermedia le interrogazioni tra operatori. Attraverso il server è possibile verificare, all'occorrenza, i dati di ogni chiamata. Ogni operatore può quindi controllare se i parametri ottenuti dall'interrogazione sono coerenti con la chiamata che si trova a gestire.

In caso contrario, la chiamata può essere bloccata.

[*Facile da implementare e sufficientemente veloce da non interferire con i tempi di chiamata*]

Proxy Server: esempio di possibile implementazione



Thank You!

Defend. Inform. Evolve.

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo aggiuntivo al tavolo tecnico

Spettabile
AGCOM
Direzione Tutela dei Consumatori

Centro Direzionale, Isola B5 - "Torre Francesco"

80143 - Napoli

e.a.

Giovanni Santella - Direttore

Massimiliano Carlomagno

Inviata tramite posta elettronica (PEC) all'indirizzo: agcom@cert.agcom.it

Omissis

Oggetto: Consultazione pubblica di cui alla delibera n. 457/24/CONS - Osservazioni rispetto alle soluzioni relative al blocco delle chiamate mobili in discussione al Tavolo Tecnico

Si fa seguito alla riunione del Tavolo Tecnico del 15 aprile u.s. per esprimere alcune considerazioni relativamente la soluzione attualmente in discussione per il blocco delle chiamate provenienti su interfacce internazionali con CLI mobile nazionale.

Come si è avuto modo di esprimere nel corso delle precedenti riunioni e nei propri contributi scritti, la soluzione definita nell'ambito del Tavolo Tecnico preliminare non trova concordi le scriventi società apparendo:

- **estremamente complessa da attuare:** essa richiede una serie di attività propedeutiche tra le quali la stipula di un accordo quadro con gli operatori mobili e l'implementazione di un numero di connessioni per ciascuno degli operatori assegnatari di numerazioni mobili che, per ragioni di sicurezza delle reti, potrebbero richiedere necessariamente il coinvolgimento di una terza parte, con un evidente aggravio dei costi ed allungamento dei tempi necessari per la sua operatività;
- **ancora in via di definizione sotto il profilo di alcuni aspetti rilevanti** per poterne definire tempi di implementazione, sostenibilità economica per tutti gli operatori presenti sul mercato ed efficacia in termini di contrasto del fenomeno del CLI spoofing.

In grado di produrre un **impatto competitivo,** di cui si dovrà tener conto, **nella fornitura dei servizi di transito** da parte degli operatori attivi esclusivamente nel segmento fisso del mercato.

Le scriventi società, pertanto, suggeriscono nuovamente di voler analizzare soluzioni già implementate con successo in altri paesi europei, quale quella belga, basate sull'utilizzo dell'HRN (Home Routing Number). Tali soluzioni, basandosi su logiche **di instradamento già oggi usate dagli operatori mobili per la gestione delle chiamate in roaming** risulterebbero, difatti, di immediata attuazione ed efficaci per garantire un rapido contrasto del CLI spoofing proveniente dall'utilizzo di numerazioni mobili. Esse risulterebbe altresì sostenibili dal punto di vista dei costi per tutti gli operatori presenti sul mercato, costituendo inoltre un rimedio proporzionato rispetto all'entità del traffico mobile legittimo che ad oggi transita sulle interfacce internazionali.

Nel corso della riunione del 15 aprile si è difatti avuto modo di apprendere che per le tecnologie 4Ge 5G il traffico degli utenti in roaming è gestito esclusivamente tramite Home Routing, non transitando attraverso le interfacce internazionali degli operatori di transito. Per le reti 2G e 3G le chiamate in roaming vengono invece gestite tramite local routing (transitano dalle interfacce internazionali) solo per quei paesi per il quali non esistono i cosiddetti accordi CAMEL con gli operatori della rete ospitante.

Dunque, in assenza di tecnologie 2G e 3G l'operatore di transito potrebbe bloccare tutte le chiamate provenienti dalle interfacce internazionali con CLI mobile nazionale senza prevedere alcuna eccezione.

Considerando che le suddette tecnologie rappresentano tecnologie obsolete ed in via di spegnimento (in Italia i principali operatori mobili hanno già proceduto allo spegnimento della rete 3G e diversi operatori europei ed extraeuropei hanno annunciato piani di spegnimento previsti tra il 2025 ed il 2030[1]) appare ancora più opportuno valutare gli oneri connessi alla soluzione proposta rispetto al traffico di utenti in roaming che effettivamente transita attraverso le interfacce internazionali. Sarebbe a tal riguardo auspicabile che nell'ambito del Tavolo Tecnico venissero condivise le percentuali di traffico in roaming che gli operatori mobili registrano sulle tecnologie 2G e 3G. Ciò al fine di garantire la proporzionalità della soluzione individuata.

In definitiva, anche alla luce dei chiarimenti ricevuti nel corso dell'ultima riunione del Tavolo Tecnico, una soluzione basata sull'HRN appare:

in linea con i principi della proporzionalità, efficienza e certezza dell'azione regolamentare in quanto garantisce la rapida applicazione delle misure di contrasto al fenomeno del CLI spoofing a tutela dell'utente finale rendendo al contempo sostenibile la soluzione per tutti gli operatori presenti sul mercato;

[1] Cfr BEREC report on 2G/3G phaseout practics and challenges and NG.121 2G-3G Sunset Guidelines

semplice da implementare sia per gli operatori mobili che per gli operatori di rete fissa in quanto:

- basata su logiche già oggi utilizzate per la gestione delle chiamate in roaming
- non richiede la stipula di alcun accordo tra operatori di transito ed operatori mobili né tantomeno la predisposizione di connessioni dedicate per le attività di query

in grado di tutelare la gestione del traffico legittimo

Si chiede pertanto che Codesta Autorità, prima di procedere all'approvazione della soluzione definitiva, voglia svolgere un ulteriore approfondimento relativamente a soluzioni alternative rispetto a quella proposta dal Tavolo Preliminare ed attualmente in discussione, basate su logiche già conosciute ed in parte implementate dagli operatori, quale quella basata sull'HRN.

Restando a disposizione per qualsiasi ulteriore chiarimento o informazione dovesse ritenersi necessaria si inviano Cordiali saluti.

omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo aggiuntivo al tavolo tecnico

Osservazioni al Tavolo tecnico AGCOM per la definizione delle modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Omissis

18 aprile 2025

Innanzitutto, approfittiamo dell'occasione per ringraziare l'Autorità per aver organizzato il Tavolo tecnico sulle soluzioni di contrasto al CLI spoofing estendendo la partecipazione anche a soggetti non del settore delle telecomunicazioni, come le Associazioni scriventi e alcuni operatori. Le finalità del Tavolo e quanto discusso con tutti gli stakeholder presenti rappresenta la forte volontà di trovare una soluzione efficace al problema che ha ormai raggiunto un livello intollerabile per i cittadini e che ha impatti negativi molto forti per gli operatori che operano corretti.

In termini generali, riteniamo la proposta posta in consultazione idonea ad affrontare le diverse casistiche di chiamate con prefisso italiano ma provenienti dall'estero, che come è stato confermato nella riunione del rappresentano la quasi totalità (il 98% circa) delle chiamate attualmente oggetto di spoofing.

Dal punto di vista delle tempistiche implementative, la proposta in consultazione prevede che le misure di blocco siano applicate prioritariamente in una prima fase sui numeri diversi dai mobili (non standard ITU, fissi geografici e non), mentre solo in una seconda fase anche sui numeri mobili. Dalle verifiche fatte dai nostri associati sulle segnalazioni ricevute, però, emerge nettamente come che **la quasi totalità delle chiamate moleste provengono da numeri mobili non richiamabili**.

Per questo motivo, **ribadiamo come fondamentale che l'Autorità diriga prioritariamente i propri interventi di contrasto al CLI spoofing nei confronti di questi numeri, e quindi auspichiamo che il blocco dei numeri mobili, insieme a quello dei numeri fissi e non standard ITU, sia implementato immediatamente a valle della Delibera e già entro la metà dell'anno**.

Quantomeno, riteniamo **fondamentale che siano attuate da subito e contestualmente alle misure di blocco dei numeri diversi da mobili anche quelle mirate contro i numeri mobili non assegnati**. Se abbiamo compreso correttamente la proposta tecnica emersa nel Tavolo, per i numeri mobili non assegnati si prevede una attività di controllo/blocco in capo ai carrier internazionali sulla base di informazioni note ex ante (es. l'assegnazione o meno del numero) e considerato che questo processo sarebbe sostanzialmente analogo a quello relativo ai numeri diversi dai mobili (in cui i carrier internazionali bloccano numeri inesistenti), riteniamo ragionevole che i due set di misure abbiano le medesime tempistiche di adozione.

Nel caso si volesse confermare una modalità di azione in fasi, proponiamo che **si potrebbe dedicare la seconda fase all'implementazione della misura di blocco dei numeri mobili assegnati ma oggetto di spoofing** (più complessa da realizzare, dato che dovrebbe prevedere scambi di informazioni in tempo reale tra carrier internazionali ed operatori nazionali, es. su roaming).

In conclusione, e con particolare riferimento alla possibilità che aumenti il numero di chiamate spoofing che nascono direttamente in Italia su rete VOIP e senza transito attraverso i carrier internazionali (a oggi ancora numericamente limitata), ribadiamo, come fatto anche dagli altri soggetti presenti, l'importanza dell'attività di **controllo e monitoraggio sistematico da parte dell'Autorità** su tutti gli operatori telefonici relativamente al rispetto della normativa nazionale sul divieto di alterazione del numero telefonico.

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo aggiuntivo al tavolo tecnico

Omissis

Omissis

Buona sera.

Omissis

Si ritiene che la soluzione Home Routing basata su Camel non sia comparabile nell'efficacia con quella basata su query discussa nel tavolo tecnico e presenta le seguenti problematiche:

- anche dove è attivo Camel l'attuale gestione delle chiamate è in Local Breakout e si tratterebbe di intervenire sui servizi CAMEL di Omissis che gestiscono il traffico originato all'estero dai nostri clienti per modificarne il trattamento con le complessità e tempistiche associate e con la rilevante disottimizzazione di costringere il tromboning sulla rete mobile home italiana; in particolare tutte le chiamate interne al paese estero e originate all'estero e destinate in altri paesi esteri, anziché risolversi all'interno del paese estero visitato o direttamente tra i paesi esteri di origine e destinazione, sarebbero instradate prima verso l'Italia e poi da qui di nuovo verso il paese estero. Sarebbe una soluzione da analizzare e normare e poi implementare con tempistiche da valutare.
- In assenza di Camel attivo ed assenza di home routing attivo il cliente in roaming all'estero, in caso di effettuazione del blocco delle chiamate che arrivano al carrier internazionale con CLI mobile, non potrà più chiamare l'Italia. Risulta che in Belgio, in questo caso, si è proceduto all'anonimizzazione del CLI e non al blocco con la conseguenza che le eventuali chiamate spoofate continuano ad arrivare agli utenti; tale soluzione non si ritiene quindi realmente efficace.
- I tempi di adeguamento per la soluzione basata su Home routing non sono brevi e richiedono l'avvio di nuove analisi tecniche per identificare i tempi e costi connessi. In via preliminare si rileva che i tempi e costi non sono per Omissis inferiori a quelli della soluzione basata su query individuata con gli altri operatori nel tavolo tecnico AGCom.

Omissis

Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo aggiuntivo al tavolo tecnico

Osservazioni di Omissis in merito ad alcuni elementi emersi nell'ambito dell'incontro del tavolo tecnico presso AGCOM del 15.04.2025

A) Diffusione del protocollo Camel nel mondo

- Relativamente ai dati di diffusione del protocollo Camel nel mondo al momento non si dispone di un report ufficiale. Gli operatori scriventi potranno rispondere singolarmente in merito agli accordi Camel stipulati dagli stessi.
- In ogni caso deve essere evidenziato che basta un solo operatore di paese estero che decide di non utilizzare il Camel per vanificare soluzioni basate su questo protocollo.
- Ad oggi risulta che diversi operatori esteri non utilizzano Camel e non ci sono strumenti normativi né leve contrattuali per imporre l'utilizzo di tale protocollo.

B) Informazioni sull'efficacia o meno della soluzione antispoofing implementata dall'autorità Autorità belga (se ne abbiamo)

- Gli operatori scriventi non hanno informazioni ufficiali sull'efficacia o meno della soluzione definita dall'Autorità Belga implementata peraltro da pochi mesi (in vigore dal dicembre 2024).
- Da informazioni tuttavia reperite informalmente da contatti diretti delle scriventi società con gli operatori belgi, risulta che nel caso delle numerazioni mobili la soluzione belga prevede l'anonimizzazione delle chiamate consegnate al carrier internazionale e NON il blocco in quanto per come è strutturata non riesce a discriminare se la chiamata è lecita o meno. Infatti il carrier internazionale non può sapere se il paese di origine dispone della funzionalità CAMEL o meno.
- La soluzione implica il transito di tutte le chiamate originate all'estero dai clienti mobili attraverso la rete home del numero originante, con il conseguente inoltro a destinazione con CLI valido, con complessità nella definizione, tempi di implementazione non stimabili ad oggi e disottimizzazione nell'utilizzo delle risorse.

C) Impatti in caso di Roaming VolTE/4G in modalità Local Break out.

- Gli operatori scriventi evidenziano innanzi tutto che *(…) the LBO option is seen as obsolete and was recently deprecated in GSMA specifications.*

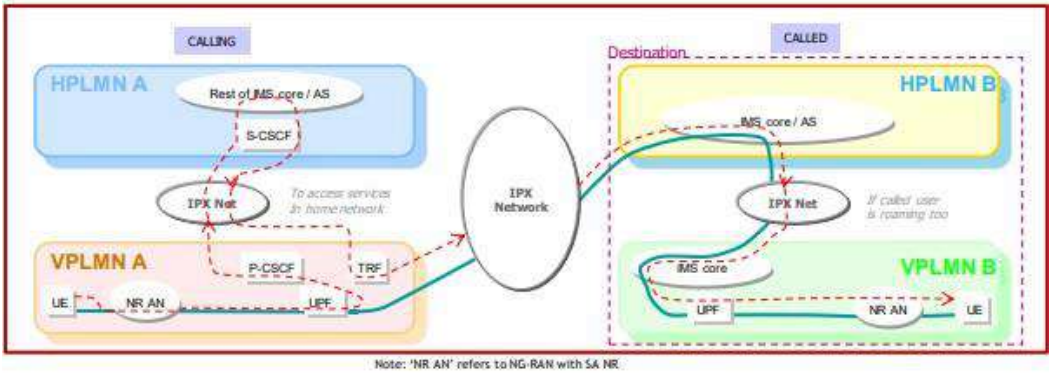
IR.65-v36.0.pdf

- Gli operatori scriventi non utilizzano LBO e non pensano di utilizzarla in futura.

- Inoltre, è bene evidenziare che LBO si divide in due tipologie:
    - LBO-HR (applica l'Home Routing
    - LBO-VR (non applica l'Home Routing).
- Nel caso LBO-HR si ha il medesimo comportamento dell'architettura VolTe 4G S8HR quindi tale situazione è coerente con l'indicazione di blocco delle chiamate in risposta alla query effettuata dal Carrier internazionale Autorizzato in Italia.
- Nel caso LBO-VR le chiamate (SIP) vengono consegnate agli operatori italiani tramite carrier internazionali (come le chiamate voce in modalità 2G/3G).

  Premesso che ad oggi nessuno degli operatori scriventi utilizza questa modalità, il problema non si pone.

  Infatti, nel caso ci fossero operatori che utilizzassero tale modalità LBO-VR tali operatori dovrebbero comportarsi in modo congruente e dovrebbero rispondere NON BLOCCA all'interrogazione API effettuata dal Carrier Internazionale autorizzato in Italia previa verifica della presenza in roaming VoLTE LBO-VR del numero.
- Di seguito due figure che mostrano le architetture LBO.



Note: 'NR AN' refers to NG-RAN with SA NR

Figure 2A-5: Control and User Plane Routing – LBO-VR

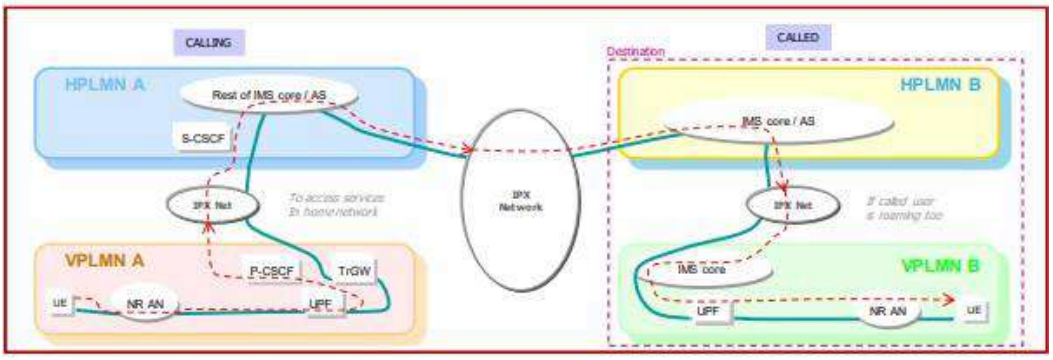


Figure 2A-6: Control and User Plane Routing

D) Nota esplicativa sulla slide 10 della presentazione circolata da AGcom il 15.04.2025

Nella tabella seguente è riportata descrizione grafica che mostra che il controllo da effettuare su HLR è l'unico necessario in quanto le chiamate da Bloccare o non bloccare sono in linea con lo stato di registrazione del cliente in 2G/3G presente in HLR.

Descrizione	HLR	HSS	Descrizione esito	Esito API
	2G/3G	4G		
Utente registrato all'estero 2G/3G/4G	Registrazione estera	registrazione estera	Le chiamate devono passare	NON BLOCCA
Utente registrato all'estero 2G/3G	Registrazione estera	Non registrato (*)	Le chiamate devono passare	NON BLOCCA
Utente registrato all'estero in rete solo 2G/3G (**)	Registrazione estera	Registrato in Italia	Le chiamate devono passare	NON BLOCCA
Utente registrato all'estero solo 4G (senza "dual attach")	Non registrato (*)	registrazione estera	La chiamata deve essere bloccata	BLOCCA
Utente registrato in Italia 2G/3G	Registrato in Italia	Non registrato (*)	La chiamata deve essere bloccata	BLOCCA
Utente registrato in Italia 2G/3G/4G (con "dual attach")	Registrato in Italia	Registrato in Italia	La chiamata deve essere bloccata	BLOCCA
Utente spento	Non registrato (*)	Non registrato (*)	La chiamata deve essere bloccata	BLOCCA

(*) se non spento, dopo lo scadere del timer di registrazione. In ogni caso non influente per l'esito delle transazioni.

(**) caso di un cliente italiano che va in roaming in una rete estera SOLO 2G/3G: in HSS potrebbe risultare ancora la registrazione in Italia.

In sostanza la tabella riportata mostra perché ai fini dei blocchi riportati nella slide 10 è necessario dettagliare nel modo riportato nella slide e non è sufficiente scrivere che il Blocco è effettuato quando il cliente "*Non è registrato all'estero*" o quando "*il cliente è registrato in Italia*".

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo aggiuntivo al tavolo tecnico

Risposta Omissis alla richiesta informazioni AGCOM del 16.04.2025

OMISSIS

OMISSIS

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Omissis

Contributo al tavolo tecnico

Spett.le
Autorità per le Garanzie nelle Comunicazioni
Via Isonzo, 21/b
00198 Roma
All'attenzione del responsabile
del procedimento ***Ing. Giovanni Santella***

Omissis

Oggetto: Nota integrativa – Riunione tecnica AGCOM del prossimo 23 aprile 2025 (Delibera n. 457/24/CONS)

La scrivente **Associazione Omissis-** fa riferimento alla prossima riunione tecnica indetta da codesta Autorità in data 23 aprile 2025, in merito ad eventuali quesiti o perplessità riguardanti le specifiche delle API.

Nell'ambito delle misure anti-spoofing del CLI, la soluzione attuale in discussione prevede l'uso di interrogazioni API in tempo reale tra operatori per identificare chiamate potenzialmente falsificate. In particolare, nei casi di chiamate internazionali entranti con un CLI mobile nazionale italiano, i carrier internazionale autorizzati in Italia interrogano tramite API l'operatore mobile italiano assegnatario del numero, al fine di verificare se la chiamata sia lecita o debba essere bloccata. Tale meccanismo mira a tutelare gli utenti finali dalle frodi telefoniche (spoofing del numero chiamante) garantendo che il numero visualizzato sia affidabile.

Nel documento preparatorio attuale (slide 12 della *"Proposta soluzioni spoofing versione finale del 15/04/2025"*), ai commi e) ed f) è indicato che, in caso di superamento dei limiti di interrogazioni API concordati, **i carrier internazionale autorizzati in Italia non debbano bloccare le chiamate**, ricevendo codici di errore 429 o 509 che segnalano la condizione di *overload*. Questa misura è pensata per salvaguardare l'integrità delle reti evitando carichi eccessivi sui sistemi di interrogazione. Tuttavia, **Omissis** – in qualità di stakeholder del settore – ritiene tale approccio non accettabile in quanto rischia di indebolire l'efficacia dei filtri anti-spoofing e di creare potenziali falle sfruttabili da attori malintenzionati.

Alla luce di queste preoccupazioni, si presenta di seguito una proposta alternativa **tecnica e regolamentare** che persegue un duplice obiettivo: da un lato **minimizzare le situazioni in cui le chiamate non vengono bloccate a causa di limiti tecnici**, dall'altro **garantire la sostenibilità e l'efficienza per gli operatori mobile** attraverso misure di resilienza (scalabilità, caching, rate shaping, ecc.).

Criticità della soluzione attuale

L'attuale soluzione (commi e) ed f) della slide 12) prevede una modalità di *fail-open*: se l'operatore interrogato non è in grado di rispondere alle query API oltre una certa soglia (per carico eccessivo), viene inviato al carrier richiedente un codice di errore (429 Too Many Requests o 509 Bandwidth Limit Exceeded) che **equivale a un'indicazione di "NON BLOCCARE" la chiamata** sospetta. Questa impostazione presenta diverse criticità:

- **Indebolimento dei filtri nei momenti critici:** Proprio quando il volume di chiamate (e potenzialmente di tentativi di spoofing) è massimo, il sistema attenua la protezione. Un malintenzionato potrebbe sfruttare tale finestra generando un sovraccarico di interrogazioni per costringere il sistema a inviare codici 429/509, permettendo il passaggio di chiamate spoofing che altrimenti sarebbero bloccate. Ciò crea una vulnerabilità prevedibile nei filtri anti-spoofing.
- **Incoerenza nella tutela degli utenti:** Gli utenti potrebbero trovarsi esposti a chiamate fraudolente proprio nelle fasce di picco di traffico o in condizioni di stress della rete, vanificando in parte il beneficio della regolamentazione. L'efficacia percepita del meccanismo di blocco ne risulterebbe ridotta, minando la fiducia nell'intero sistema di protezione.
- **Rischio di comportamento non uniforme tra operatori:** Lasciare ai singoli operatori la facoltà di inviare un "non blocco" in caso di overload può portare a discrepanze nelle implementazioni. Alcuni operatori potrebbero applicare soglie più conservative o reagire diversamente all'aumento di traffico, causando difformità nel trattamento delle chiamate sospette. Ciò complicherebbe anche la conformità regolamentare e il monitoraggio del rispetto delle regole.
- **Mancanza di garanzie su tempi e recupero:** L'attuale soluzione non specifica chiaramente come e quando il sistema dovrebbe tornare allo stato normale dopo un evento 429/509, né prevede retry immediati. Questo potrebbe comportare che, dopo un primo rifiuto della query, ulteriori chiamate nel frattempo passino senza controllo, prolungando l'esposizione al rischio. Inoltre, l'assenza di tentativi di ripetizione (*no retry*) sul codice 429 impedisce di verificare se il sovraccarico fosse transitorio.

In sintesi, la strategia di fail-open per motivi tecnici sacrifica la sicurezza (blocco dello spoofing) sull'altare della stabilità di rete, invece di ricercare soluzioni che **garantiscano sia la resilienza dell'infrastruttura sia la continuità della protezione anti-spoofing**. È quindi necessario ripensare questo aspetto introducendo meccanismi che **evitino il più possibile di dover rinunciare al blocco** delle chiamate illecite, pur mantenendo le reti

operative entro parametri sostenibili.

Proposta alternativa

La proposta alternativa si basa sul principio del **fail-safe** (o *fail-closed* moderato), affiancato da potenziamenti infrastrutturali e accorgimenti tecnici per gestire in modo intelligente i picchi di traffico. Invece di prevedere di default il **non-blocco** delle chiamate in caso di superamento delle soglie di interrogazione, si propone di **rafforzare l'intera catena di controllo** affinché tali condizioni siano rare e comunque gestite senza compromettere la tutela degli utenti. Di seguito gli elementi chiave della proposta:

- **Dimensionamento e scalabilità adeguati:** Ogni operatore mobile dovrà concordare con i carrier internazionale autorizzati in Italia e implementare un dimensionamento "sostenibile" delle piattaforme di query **ampiamente sufficiente a gestire i carichi di picco** previsti. Ciò implica:
    - Analisi dei volumi di traffico storici e stima dei casi peggiori (es. campagne di chiamate massicce) per determinare la **capacità necessaria (numero di query al secondo/minuto)** per ciascuna interfaccia API tra carrier internazionali autorizzati in Italia e operatori mobili.
    - **Margine di sicurezza**: aggiungere un margine (es. +20%/30%) oltre il picco massimo stimato, in modo da coprire variazioni impreviste o crescita del traffico, evitando di raggiungere le soglie critiche in condizioni ordinarie.
    - **Scalabilità orizzontale/verticale**: predisporre architetture scalabili (es. istanze server aggiuntive, cloud elastico, load balancer) tali che, al crescere del carico, le risorse backend per le API possano essere aumentate dinamicamente o in modo rapido. In questo modo, anche in caso di eventi eccezionali, il sistema può temporaneamente potenziare la capacità di risposta senza andare in sovraccarico.
    - Verifiche periodiche e stress test congiunti tra carrier internazionale autorizzati in Italia e operatori mobile per tarare il dimensionamento e aggiornare le risorse in base all'evoluzione del traffico reale.
    - **Predisposizione di basi di dati dedicate e parallele a quelle tradizionali**, idonee ad un elevato throughput e facilmente scalabili orizzontalmente, da aggiornare su base temporale (es. ElasticSearch, Apache Cassandra o similari)
- **Ottimizzazione delle interrogazioni (caching):** Per ridurre il volume di query effettivamente necessario e alleggerire il carico:
    - Implementare un **meccanismo di caching** lato operatore mobile interrogato: se più chiamate in arrivo interrogano in breve tempo la stessa informazione

(es. lo stesso numero CLI), la risposta precedente può essere riutilizzata per un intervallo temporale limitato (ad esempio pochi secondi), evitando interrogazioni ripetitive inutili. Questo è particolarmente utile in caso di ondate di chiamate spoofing che spesso riutilizzano gli stessi numeri chiamanti.

- **Rate shaping e gestione dei picchi:** In luogo di rispondere con un errore immediato di sovraccarico, introdurre meccanismi di smorzamento del traffico di interrogazione:
    - **Coda controllata delle richieste:** all'avvicinarsi della soglia di capacità, l'operatore interrogato può mettere in coda temporaneamente alcune query invece di rifiutarle, gestendole con qualche millisecondo di ritardo. Questo *buffer* consente di assorbire picchi brevissimi senza perdere richieste. È necessario coordinarsi sui timer di segnalazione call setup (ISUP/SIP) affinché un piccolo ritardo (es. nell'ordine di 100-500 ms aggiuntivi) sia tollerabile senza causare cadute chiamata; in pratica, un leggero **allungamento del tempo di setup** della chiamata viene accettato per privilegiare l'esito certo della query.
    - **Prioritizzazione intelligente:** se il volume di chiamate sospette è tale da dover comunque scartare parte delle interrogazioni, si può introdurre una logica di prioritizzazione. Ad esempio, dare priorità alle query relative a pattern di traffico noti come più rischiosi (es. chiamate da determinati paesi fonte di molte frodi, o utilizzo ripetuto di numeri non allocati) e gestire secondariamente i casi ritenuti a minor rischio. In questo modo, anche in condizioni estreme, **le chiamate più probabilmente fraudolente continuano ad essere filtrate** per prime.
    - **Rate limit per singolo carrier adattivo:** invece di un taglio netto sul limite predefinito, si potrebbe adottare un sistema adattivo in cui il rate di interrogazioni accettate da ciascun carrier internazionale autorizzato in Italia viene modulato in base al suo profilo di traffico e alla situazione. Ad esempio, se un particolare carrier internazionale autorizzato in Italia sta inviando volumi eccezionalmente alti di query, l'operatore mobile potrebbe iniziare a rispondere con un leggero ritardo o segnalazioni di *slow-down* (senza però autorizzare il passaggio delle chiamate sospette), spingendo il carrier magari a **diradare leggermente l'invio delle chiamate** in ingresso (es. applicando a sua volta un rate shaping sugli inoltri delle chiamate internazionali con CLI italiano). Questo richiede cooperazione tra le parti, ma aiuterebbe a evitare il collasso del sistema senza aprire falle di sicurezza.
    - **Meccanismi di fallback temporaneo (fail-safe invece di fail-open):** Nel caso in cui, nonostante le misure precedenti, si verifichi una condizione di

sovraccarico tale da impedire la risposta alle query entro tempi utili, la gestione predefinita dovrà **mirare comunque a massimizzare la tutela anti-spoofing**:

  - **Fallback con esito predefinito di sicurezza:** Se una query verso l'operatore mobile *timeout* o eccede il tempo limite, la proposta prevede di considerare la chiamata sospetta **da bloccare in via prudenziale**, anziché lasciarla passare. Questo garantisce un comportamento *fail-safe*: meglio bloccare temporaneamente una chiamata lecita (**che potrà eventualmente essere riprovata**) piuttosto che lasciare transitare una chiamata fraudolenta. Un esempio concreto di come un sistema di rete decidere se bloccare temporaneamente alcune chiamate lecite per garantire la stabilità complessiva è quello delle **reti congestionate** durante eventi come concerti o partite di calcio, dove le risorse di rete non sono sufficienti per gestire tutte le richieste. In questi casi, la rete preferisce **rifiutare temporaneamente** alcune chiamate legittime per evitare che il sistema collassi, in modo da preservare la stabilità per tutti. Allo stesso modo, nel caso delle chiamate sospette, il **fallback con esito predefinito di sicurezza** dovrebbe preferire il **blocco della chiamata sospetta**, piuttosto che permettere che una chiamata fraudolenta passi. Tale scelta andrà esplicitamente autorizzata normativamente, in quanto comporta possibili blocchi di chiamate lecite in scenari di errore tecnico, ma offre maggiore garanzia di protezione.

- **Soglie adattive e monitoraggio continuo:** La definizione delle soglie di traffico (numero massimo di query al secondo per singolo rapporto carrier<>operatore e totale sistema) dovrebbe essere **dinamica e rivista periodicamente**:
  - **Adattività basata sul carico:** Implementare algoritmi che adeguino automaticamente alcune soglie in base all'andamento temporale del traffico. Ad esempio, se si riscontra che determinati orari o giorni della settimana presentano volumi più elevati, i sistemi possono pre-scalare risorse e innalzare limiti di allerta in quei periodi, riducendoli in fasce più tranquille. Questo evita rigide limitazioni fisse che potrebbero essere troppo prudenti in alcuni casi o insufficienti in altri.
  - **Monitoraggio e reportistica in tempo reale:** Sia i carrier internazionali sia gli operatori mobili dovranno dotarsi di strumenti di monitoraggio h24 delle query e delle relative risposte. **Dashboard di controllo** mostreranno in tempo reale il tasso di utilizzo delle API rispetto ai limiti concordati, generando alert al superamento di determinate soglie (es. 80% della capacità) così da permettere interventi proattivi (scaling manuale aggiuntivo, blocco di flussi anomali, ecc.) *prima* di arrivare al punto di rottura.

- **Revisione periodica delle performance:** In sede tecnica (es. tavoli periodici mensili o trimestrali), gli operatori dovrebbero condividere statistiche sulle query effettuate, sui casi di overload evitati o occorsi, sui tempi di risposta medi e massimi, e su eventuali chiamate bloccate per fail-safe. Questa collaborazione consentirà di identificare colli di bottiglia, aggiornare i requisiti di capacità e perfezionare gli algoritmi di soglia adattiva. In pratica, il sistema normativo rimane **flessibile e aggiornabile** sulla base dell'evidenza operativa.

In sintesi, la proposta alternativa elimina l'idea che il superamento dei limiti tecnici debba automaticamente tradursi in un via libera alle chiamate sospette. Piuttosto, concentra gli sforzi sul **potenziare l'infrastruttura e ottimizzare i meccanismi** per evitare di oltrepassare tali limiti, e sul definire comportamenti di fallback che **preservino il più possibile la funzione di blocco**. Questo richiede sia interventi tecnici (upgrade sistemi, sviluppo software per caching, etc.) sia coordinamento regolamentare tra gli operatori per stabilire procedure comuni e chiare in condizioni eccezionali.

Monitoraggio delle performance e rating di affidabilità degli operatori mobili

Ogni operatore mobile dovrà fornire periodicamente all'Autorità un **report dettagliato** relativo ai casi di errore 429/509 (limitazioni di traffico o sovraccarico delle risorse) e alla **gestione di tali eventi**. Questi report serviranno come base per **creare un sistema di rating** che valuta la capacità di ogni operatore mobile di **proteggere i propri clienti da chiamate fraudolente** (spoofing), in particolare quelle provenienti dall'estero.
Il sistema di **rating** assegnerà un punteggio di **affidabilità e protezione** a ciascun operatore mobile, prendendo in considerazione:

- La **frequenza** e l'**impatto** dei casi di 429/509.
- La **prontezza e l'efficacia** con cui l'operatore gestisce questi eventi.
- La **capacità di bloccare** le chiamate spoofing senza compromettere la qualità del servizio.

Questo **ranking di affidabilità** sarà reso pubblico e monitorato dalle **autorità competenti**, fungendo da strumento di **trasparenza** e da **incentivo** per gli operatori a **migliorare continuamente le loro infrastrutture**. Un rating elevato rifletterà l'impegno dell'operatore nel garantire **la sicurezza degli utenti** e nella **prevenzione delle frodi telefoniche**, mentre un rating basso potrebbe suggerire la necessità di interventi per migliorare la protezione del sistema e dei clienti

Conclusioni

La proposta alternativa delineata intende **chiudere le falle** presenti nella soluzione attuale, assicurando che i filtri anti-spoofing rimangano efficaci anche in condizioni di stress. Attraverso un mix di soluzioni tecniche (scalabilità, caching, sistemi di fallback) e misure regolamentari (obblighi di dimensionamento, cooperazione tra operatori, autorizzazione al blocco prudenziale di sicurezza), si persegue un sistema in cui il superamento dei limiti tecnici **non coincida più con la sospensione delle tutele** per gli utenti.

Certi della Vostra attenzione, si porgono distinti saluti.

Roma 22 Aprile 2025

Omissis

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera 457/24/CONS

Resoconti sintetici delle riunioni del tavolo tecnico:

- 27 marzo 2025
- 1° aprile 2025
- 3 aprile 2025
- 9 aprile 2025
- 15 aprile 2025
- 23 aprile 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Resoconto sintetico della riunione del tavolo tecnico del 27 marzo 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera n. 457/24/CONS

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui all'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Resoconto sintetico della riunione del 27 marzo 2025

Il giorno 27 marzo 2025 alle ore 11:30, si è tenuta, presso la sala Angrisani della sede di Roma dell'Autorità e in videoconferenza per i partecipanti che ne hanno fatto richiesta, una riunione del tavolo tecnico convocato nell'ambito del procedimento avviato con la delibera n. 457/24/CONS, con l'obiettivo di discutere le modalità implementative delle misure tecniche di blocco di cui ai commi 1 e 2 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS. In particolare, l'incontro mirava a raccogliere osservazioni sulle specifiche tecniche proposte, allegate alla convocazione del tavolo tecnico.

L'incontro ha visto la partecipazione delle principali associazioni dei consumatori, associazioni di imprese, operatori di telecomunicazioni (TLC) e altri attori rilevanti, tra cui esperti e operatori di altri settori direttamente coinvolti nella questione del CLI spoofing, oltre che dei rappresentanti dell'Autorità.

L'elenco delle società partecipanti è riportato in allegato.

AGCOM, dopo aver ringraziato i presenti per la nutrita partecipazione, ha aperto la sessione illustrando brevemente il contenuto dell'articolo 8 della delibera, che riguarda le misure per garantire la trasparenza e la tutela degli utenti finali in relazione alle chiamate con CLI modificato. Ha ceduto quindi la parola ai partecipanti, che hanno potuto esprimere le proprie opinioni riguardo le misure tecniche proposte e finalizzate a contrastare il fenomeno del CLI *spoofing*.

Omissis ha espresso alcuni dubbi in merito alla soluzione prospettata. Nel merito, l'associazione teme che, dopo l'implementazione della prima delle due fasi previste, il fenomeno dello spoofing potrebbe passare a utilizzare numerazioni attive di utenti ignari; chiede chiarimenti sui soggetti che rientrano nella classificazione di "Carrier Internazionale autorizzato in Italia" e sull'inquadramento di tali soggetti come "operatori", dunque sull'applicabilità della delibera nei loro confronti; chiede sesia stato considerato il fenomeno dello spoofing messo in atto tramite chiamate VoIP immesse nelle reti 4G in tecnologia VoLTE.

Omissis ritiene che i blocchi relativi alle due fasi previste debbano essere implementati contemporaneamente. L'associazione segnala inoltre che, per quanto riguarda lo *spoofing* originato in ambito nazionale, le disposizioni previste dal Piano Nazionale di Numerazione per la correttezza e la salvaguardia del CLI non vengono applicate da tutti gli operatori.

Alcuni degli **operatori** che hanno formulato la proposta in discussione hanno fornito chiarimenti in merito ai punti sollevati dall'associazione.

Con riferimento al VoLTE, è stato precisato che una chiamata VoLTE originata all'estero non passa attraverso le interfacce internazionali, ma transita direttamente nella rete dell'operatore

dell'utente. Di conseguenza, una chiamata con CLI di rete mobile che giunge alle interfacce di connessione internazionali, e che è associata a un utente in roaming su rete 4G/VoLTE, può essere sicuramente classificata come *spoofing*. Inoltre, stanti gli efficaci meccanismi di sicurezza delle reti 4G, le chiamate originate su rete 4G/VoLTE che giungono all'operatore nazionale non possono essere soggette a *spoofing*. In merito alle chiamate VoIP unmanaged, viene chiarito che queste chiamate, non generate su rete 4G, non possono essere immesse nella rete mobile bensì attraverso sistemi di originazione sul territorio nazionale, a valle di apparati gataway di conversione da VoIP a PSTN, da rete fissa. Occorre dunque fare una distinzione fra chiamate VoLTE e chiamate VoIP unmanaged.

Il problema dello spoofing basato su chiamate VoIP originate in rete dati è oggetto delle misure previste al comma 4 dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS. In proposito, è stato da più parti sottolineato il ruolo e l'efficacia della normativa sulla correttezza e inalterabilità del numero chiamante, che impone agli operatori di origine delle chiamate (inclusi quelli che ricevono le chiamate dalle reti dati) di operare un controllo sulla correttezza del CLI originato.

Riguardo alle chiamate VoIP, **Omissis** ha posto l'accento sull'importanza di controlli rigorosi da parte degli operatori di accesso evidenziando che nei servizi "*unmanaged*" spesso tale controllo manca. Evidenzia la questione di soggetti che hanno in uso la numerazione di un operatore e la utilizzano solo per le chiamate in ricezione, mentre affidano il traffico VoIP uscente a reti di altri operatori che potrebbero avere controlli meno stringenti. Concorda che il tavolo di lavoro si sta muovendo nella giusta direzione ma insiste sulla necessità di affrontare anche il fenomeno dello *spoofing* che ha origine in Italia.

Riguardo all'attuazione dei blocchi da parte dei Carrier Internazionali autorizzati in Italia, gli **operatori** hanno precisato che si tratta di soggetti con autorizzazione italiana tenuti a rispettare le leggi e le norme nazionali. Le soluzioni di blocco sulle interfacce internazionali mirano a risolvere il problema principale che le analisi hanno sempre mostrato consistere nello spoofing proveniente dall'estero. La soluzione proposta contempla tutti casi di spoofing che transitano per le interconnessioni internazionali, bloccandoli tutti.

Con riferimento alle due fasi implementative previste dalla proposta, gli **operatori** hanno chiarito che queste sono giustificate dalla diversa complessità delle misure riguardanti le chiamate internazionali con CLI fisso e con CLI mobile. Viene inoltre precisato che la prima fase prevede il blocco delle chiamate internazionali con CLI corrispondente a numerazione geografica e non geografica diversa dalla numerazione mobile, sia con riferimento e numeri assegnati che non assegnati. Pertanto, non si presenterà il problema della "migrazione" del fenomeno di *spoofing* sui numeri attivi a seguito dell'attuazione della prima fase.

Omissis, nel commentare i diversi punti di vista circa l'efficacia delle misure, anche in relazione al problema dello spostamento dello *spoofing* su tecniche diverse da quelle attuali e a quello dello *spoofing* originato in ambito nazionale, evidenzia che in problematiche complesse la soluzione non può essere definita in un unico step. Il blocco dello *spoofing* effettuato mediante chiamate transitanti dall'estero risolverà gran parte del problema, riportando la giurisdizione a livello nazionale e dando all'Autorità la possibilità di individuare e sanzionare i responsabili. L'operatore sottolinea che l'Autorità chiede di implementare rapidamente le misure di contrasto allo spoofing. Se emergeranno nuove problematiche, ci si ritroverà per trovare altre soluzioni.

Omissis ritiene che, tecnicamente, la proposta in discussione sia molto valida e che lo spoofing da Italia a Italia sia impossibile se le regole vengono rispettate e ci sono strumenti per intervenire in caso di anomalie.

Omissis chiede se sia possibile definire indicatori quantitativi (su base dati pubblica) per misurare l'efficacia delle misure ed assicurarsi che gli sforzi messi in atto per contrastare il fenomeno vadano nella giusta direzione.

Omissis apprezza l'attività di regolamentazione, ma evidenzia che qualsiasi regolamentazione sarà soggetta a tentativi di elusione da parte di soggetti intenzionati a commettere frodi. Sottolinea la maggiore gravità della clonazione di numeri appartenenti a enti che godono della fiducia dei consumatori (come uffici postali, istituti bancari), rispetto alla clonazione di numeri di privati cittadini e invita gli operatori a definire regole specifiche per creare una "*whitelist*" di numeri di istituzioni particolarmente meritevoli di fiducia, che dovrebbero essere estremamente difficili da clonare. Rileva la mancanza, nell'articolo 8, di un meccanismo per verificare costantemente i risultati e aggiornare gli standard tecnici.

Omissis ritiene che un valido indicatore di misurazione consista nel numero di chiamate bloccate, in merito al quale è prevista una reportistica per l'Autorità che quantifica le chiamate bloccate per singolo carrier internazionale e per fascia oraria.

Omissis si rende disponibile a fornire un indicatore di efficacia consistente nell'andamento del numero di frodi andate a buon fine.

Omissis conferma la disponibilità delle associazioni consumatori per il monitoraggio e le campagne di educazione. Ritiene opportuno che, oltre alle misure tecniche, si valuti la possibilità di interventi legislativi e regolamentari per impedire ai *call center* di sottoscrivere contratti telefonici senza il diretto intervento del consumatore. L'associazione ha suggerito che i consumatori dovrebbero essere tenuti a richiamare il numero telefonico ricevuto per verificare se il numero corrisponde effettivamente a un soggetto commerciale, evitando così situazioni di truffa o contratti sottoscritti in modo non consapevole. Evidenzia anch'essa l'opportunità di prestare particolare attenzione al fenomeno dell'utilizzo di numeri "sensibili" (banche, polizia e altro) nelle pratiche di spoofing.

Omissis precisa che, nella proposta in discussione, una chiamata con CLI "sensibile" proveniente dall'estero sarebbe bloccata mentre per le chiamate originate nel territorio nazionale vige una normativa di controllo molto stringente.

Omissis, entrando nel merito della proposta tecnica in discussione, commenta la slide n. 5 del documento inviato contestualmente alla convocazione del tavolo. Con riferimento all'azione preliminare di armonizzazione dei campi "PAI" e "From", ritiene sufficiente verificare i soli PAI con numerazione italiana. In aggiunta, ritiene opportuno inserire, tra le casistiche da bloccare, almeno altri due scenari: quello di un numero che inizia con "+39" seguito da un numero di distretto inesistente (non corrispondente ai distretti italiani) e quello di un numero che include un *country code* non assegnato a livello internazionale.

Passando poi a commentare la slide n. 6, con riferimento ai blocchi delle numerazioni geografiche, l'operatore ritiene ci si debba interrogare sulla modalità di gestione delle numerazioni di San Marino. Chiede inoltre di aggiungere una eccezione corrispondente al caso in cui il numero chiamato non sia italiano.

Con riferimento alla soluzione per il CLI mobile, Omissis ritiene che quella prospettata sia troppo complessa e propone una soluzione in cui l'operatore mobile "colora" le chiamate dei clienti in roaming all'estero assegnandogli un *routing number* specifico al posto del numero chiamato. Il carrier internazionale fa passare le chiamate con CLI mobile destinate ai *routing number*, le altre chiamate con CLI mobile vengono bloccate. Questa soluzione, già implementata in Belgio, eviterebbe molte interazioni intermedie per la verifica del blocco.

Omissis concorda con Omissis, sottolinea di aver implementato rapidamente e senza particolari problemi la soluzione in Belgio e si offre di fornire dati di efficacia e supporto tecnico. Riguardo ai blocchi per numeri fissi, l'operatore chiede un chiarimento sulle eccezioni previste, osservando che la raccomandazione CEPT include anche degli scenari relativi al *call forwarding* mentre nella soluzione proposta queste chiamate verrebbero bloccate.

Omissis evidenzia che la soluzione indicata da Omissis richiede un accordo che prevede l'uso del protocollo standard CAMEL fra rete visitata e rete home. Pertanto, affinché la soluzione sia applicabile in modo generalizzato, tutti gli accordi con tutte le reti visitate dovrebbero essere rivisti. È inoltre possibile che alcuni operatori non utilizzino lo standard CAMEL.

AGCOM propone di affrontare questo punto in una riunione tecnica appositamente convocata allo scopo. Nell'osservare che la soluzione "belga" richiede un accordo con tutte le reti visitate invita comunque a ragionare sugli aspetti di un obbligo regolamentare in Italia il cui rispetto è condizionato dalla buona riuscita di accordi con altri operatori all'estero.

Riguardo al *call forwarding*, **Omissis** osserva che una chiamata soggetta a inoltro non è riconoscibile con certezza sull'interconnessione internazionale in quanto la relativa informazione può non essere presente nella segnalazione, non essendo obbligatoria a livello globale. L'unica possibilità è dunque quella di bloccare anche queste chiamate perché indistinguibili in modo certo.

Nel corso dell'incontro, è emersa anche una richiesta di chiarimento riguardo ai tempi di implementazione delle soluzioni proposte. I partecipanti hanno sollevato la necessità di definire tempistiche chiare per l'adozione delle misure tecniche, così da assicurare che vengano implementate in tempi ragionevoli e con la dovuta efficacia.

A conclusione della riunione, **AGCOM** ha ritenuto la discussione ampia e costruttiva, con diversi spunti anche regolamentari e il chiarimento di diverse questioni. Ritiene utili le osservazioni e valutazioni tecniche svolte riguardanti la soluzione utilizzata in Belgio che potrà essere ulteriormente approfondita con i contributi del Tavolo. Il Tavolo tecnico comunque continuerà a lavorare sulle misure del comma 4.

Infine, **AGCOM** ha invitato tutti i partecipanti a far pervenire contributi scritti, comprese ulteriori proposte o osservazioni, al fine di arricchire il dibattito e affinare le soluzioni da adottare. L'Autorità si riserva di convocare ulteriori riunioni anche focalizzate sulle questioni aperte.

La riunione termina alle ore 13:45.

Allegato

Elenco dei partecipanti

Adiconsum
A2A
AIIP
Altroconsumo
Assocall
Assoutenti
BT
CertFIN
Codacons
Colt Technologies Service
Commify Italia
Coop Italia
Dalla Vedova Studio Legale
Edison
Elettricità Futura
Enel
Engie
Eolo
Fastweb
Fibercop
HAL Service
Iliad
Innovasemplice
Intermatica
McLink
MessageNet
NHM
Optima Italia
Postepay
Proxigas
Retelit
Sky
Studio Legale Gallotto
Tata Communications
TI Sparkle
TIM
Twilio
U.Di.Con.
Verizon Italia
Vianova
Vodafone
WindTre

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Resoconto sintetico della riunione del tavolo tecnico del 1° aprile 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera n. 457/24/CONS

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui all'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Resoconto sintetico della riunione del 1° aprile 2025

Il giorno 1° aprile 2025, alle ore 10:30, si è tenuta in videoconferenza una riunione del tavolo tecnico convocato nell'ambito del procedimento avviato con la delibera n. 457/24/CONS. La seduta ha avuto l'obiettivo di discutere le soluzioni tecniche per l'implementazione della misura prevista al comma 2 lettera c) dell'art. 8 dell'allegato B alla delibera n. 457/24/CONS, relativo al blocco delle chiamate internazionali con CLI di rete mobile.

In particolare, l'incontro ha consentito di approfondire la soluzione discussa nell'ambito della seduta del tavolo tecnico del 27 marzo 2025, proposta dall'operatore Omissis nell'ambito della stessa seduta e condivisa dall'operatore Omissis.

L'incontro ha visto la partecipazione delle principali associazioni dei consumatori, associazioni di imprese, operatori di telecomunicazioni (TLC) e altri attori rilevanti, tra cui esperti e operatori di altri settori direttamente coinvolti nella questione del CLI spoofing, oltre che dei rappresentanti dell'Autorità.

L'elenco delle società partecipanti è riportato in allegato.

AGCOM ha aperto la sessione illustrando l'obiettivo della riunione ed ha successivamente ceduto la parola ai partecipanti.

Omissis, dopo aver precisato che la soluzione da lei proposta è stata adottata in Belgio tramite un Royal Decree, ne ha illustrato gli aspetti tecnici. Questa soluzione prevede che, nella fase di instaurazione della chiamata da parte di un utente in roaming internazionale, l'operatore ospitante sostituisca il numero chiamato con un numero nazionale appartenente a un arco di numerazioni non portabili, c.d. Home Routing Number (HRN). Questa operazione viene eseguita utilizzando il protocollo standard CAMEL tra l'operatore della rete *visited* (dove l'utente in roaming è registrato) e l'operatore della rete *home* (l'operatore dell'utente).

I carrier internazionali instradano le chiamate con CLI mobile in cui il numero chiamato è un HRN verso l'operatore mobile cui è assegnato, ovvero l'operatore mobile dell'utente chiamante. Quest'ultimo verifica che l'utente sia effettivamente in roaming e che l'HRN sia valido, bloccando eventualmente le chiamate che non vengano riconosciute come valide. La corretta istaurazione della chiamata avviene quindi a seguito del ripristino, da parte dell'operatore mobile, del numero originariamente chiamato in luogo dell'HRN.

Le chiamate con CLI mobile e numero di destinazione diverso da un HRN vengono invece anonimizzate, in modo che l'utente chiamato le visualizzi originate da un numero anonimo.

Questa strategia consente di gestire i casi in cui non esiste un accordo per l'utilizzo del protocollo standard CAMEL fra l'operatore della rete *visited* e l'operatore della rete *home*, necessario per gestire il meccanismo di sostituzione del numero chiamato con l'HRN.

A parere di Omissis, l'anonimizzazione della chiamata è efficace per arginare lo spoofing e consente di evitare il rischio di bloccare chiamate legittime (effettuate da utenti in roaming registrati presso un operatore che non adotta il protocollo CAMEL).

Omissis si associa alla posizione di Omissis, evidenziando che ad oggi è l'unica soluzione per la gestione delle chiamate mobili in arrivo alle interfacce internazionali che ha implementato.

Agcom precisa che le soluzioni di anonimizzazione sono state valutate nel corso del procedimento e sono state considerate non particolarmente soddisfacenti rispetto alle esigenze di tutela degli utenti finali.

Si apre a questo punto un'ampia discussione sull'effetto dell'anonimizzazione e sull'incidenza dei casi in cui, adottando il blocco delle chiamate anche per numero chiamato diverso da un HRN, si bloccherebbero delle chiamate legittime. Questa casistica è legata al numero di operatori che non adottano il protocollo CAMEL.

Vengono espressi anche diversi punti di vista in merito alla complessità e al costo della soluzione basata su *query* verso gli operatori mobili (presentata nella seduta del tavolo del 27 marzo) rispetto a quella basata sull'HRN. Si citano anche le esperienze internazionali, in particolare quelle realizzate in Finlandia e in Repubblica Ceca, basate su un meccanismo di *query* per individuare gli utenti in *roaming*, e quella Belga, basata sull'HRN.

Omissis chiarisce che gli operatori mobili non hanno proposto la soluzione di *home routing* per due motivi principali. Il primo motivo indicato è che l'*home routing* richiede funzionalità sulle reti estere (CAMEL): non tutte le reti internazionali supportano CAMEL e una significativa porzione di reti rimarrebbe scoperta; in particolare gli accordi sono abbastanza diffusi in Europa, ma poco diffusi nel resto del mondo. Evidenzia che non è possibile intervenire sulle reti estere per obbligarle ad implementare tali funzionalità, osservando che la diffusione degli accordi CAMEL non è in crescita. Il secondo motivo indicato è che l'*home routing* renderebbe meno efficiente la gestione delle chiamate 2G/3G generate dei clienti in roaming, costringendo queste chiamate a passare inutilmente attraverso le reti nazionali. Ritiene inefficace l'anonimizzazione del CLI, in quanto le chiamate oggetto di *spoofing* arriverebbero comunque al cliente, che perderebbe visibilità sul numero chiamante e non saprebbe quale numero segnalare per tracciare l'origine delle chiamate.

Omissis si associa alle osservazioni di Omissis in merito alle limitazioni e alla non percorribilità della soluzione di anonimizzazione secondo le indicazioni attuali.

Omissis aggiunge che la complessità dell'*home routing* impatterà significativamente anche gli MVNO full, che dovrebbero implementare accorgimenti tecnici che attualmente non sono nelle loro disponibilità, con una complessità maggiore rispetto all'implementazione di un'API per esporre lo stato di roaming.

Omissis, nel condividere la posizione di Omissis e Omissis, osserva che la funzionalità di roaming, di cui si discute, è una funzionalità di rete mobile; gli obblighi connessi dovrebbero pertanto essere imposti agli operatori di rete mobile, in questo modo si accelererebbe anche il loro sviluppo

considerato che gli operatori di rete fissa non hanno incentivo a sviluppare soluzioni che non rientrano nel proprio *business*.

Omissis evidenzia il rischio elevato di anonimizzare chiamate lecite, sottolineando che lo scopo principale dello spoofing non è la richiamata, ma il contenuto della chiamata. Si dichiara a favore della soluzione basata su query con API, ritenendola più veloce e indipendente dagli operatori internazionali.

Omissis evidenzia diverse criticità relative alla proposta di utilizzare la "query" come soluzione tecnica, sottolineando la mancanza di definizioni chiare sull'allungamento del tempo di setup e l'assenza di valutazioni sull'impatto sui timer delle reti mobili, oltre alla mancata definizione del dimensionamento sostenibile delle API per gli operatori. Sostiene inoltre che il *roaming* è una funzionalità tipicamente mobile e che, senza obblighi regolamentari proporzionati, gli operatori mobili non avrebbero interesse a stipulare accordi CAMEL, lasciando l'intero onere sul transito. Riguardo al dato del 40% dei Paesi che non dispone di CAMEL, chiarisce che ciò non implica automaticamente il blocco o l'oscuramento del 40% del traffico.

Omissis evidenzia che il problema non è la percentuale di accordi CAMEL esistenti o mancanti, ma il fatto che una copertura globale CAMEL non è ipotizzabile, rendendo impossibile agire in modo certo sulle chiamate provenienti dall'estero.

Agcom richiama il contesto in cui si sta operando per la definizione delle misure *antispoofing*, caratterizzato da una elevata attenzione sul fenomeno da parte del mondo istituzionale e dei media. Questo richiede l'adozione di una soluzione, per il blocco internazionale, che copra tutte le casistiche in modo efficace e tutelante.

Omissis propone una diversa soluzione in cui sono esclusivamente gli operatori mobili a verificare gli utenti in roaming, senza bisogno di un'interrogazione da parte dei carrier internazionali. Il carrier internazionale trasferirebbe in ogni caso una chiamata con CLI mobile a un operatore di rete mobile che, qualora non fosse l'operatore di terminazione, agirebbe da operatore di transito verificando, eventualmente con la collaborazione degli altri operatori mobili, se la chiamata proviene da un utente in roaming.

L'associazione ritiene che la soluzione proposta da Omissis non fornisca le dovute garanzie.

Omissis segnala che, per permettere alle sole reti mobili di effettuare le verifiche, sarebbe necessario "colorare" il traffico internazionale, distinguendolo da quello nazionale. Tuttavia, questa procedura risulterebbe più complessa rispetto all'uso delle query: un operatore al confine potrebbe "colorare" il traffico internazionale inviandolo poi a un operatore mobile, che eseguirebbe le query con gli altri operatori mobili. Se invece la chiamata fosse destinata a un operatore fisso, quest'ultimo dovrebbe interrogare tutti gli operatori mobili, generando una complessa rete di interconnessioni. Questa ipotesi era stata analizzata ma si era optato per le query effettuate da un numero limitato di operatori di transito di frontiera, per contenere il numero di interrogazioni.

Omissis ritiene che sarebbe utile, ai fini delle operazioni di blocco, consentire agli operatori nazionali di riconoscere la provenienza del traffico internazionale, possibilità attualmente preclusa dalla specifica tecnica sull'interconnessione che, almeno per il VoIP, prevede il mascheramento dell'operatore originante con l'operatore di transito.

In proposito **Omissis** osserva che le specifiche nazionali non si applicano alle interfacce internazionali, per cui una modifica della specifica non avrebbe comunque un effetto utile. L'operatore ritiene inoltre che il traffico soggetto a spoofing debba essere bloccato quanto prima, dunque dal carrier internazionale, e non debba essere inoltrato in rete nazionale anche per motivi di sicurezza.

Anche **Omissis** ritiene che il traffico di spoofing debba essere bloccato al confine, la sua propagazione nelle reti nazionali comporterebbe infatti il rischio di non riuscire più a distinguerlo dal traffico lecito.

Omissis ritiene valida la soluzione individuata da Omissis e descrive una possibile modalità tecnica per la sua implementazione. Il carrier internazionale potrebbe inoltrare tutte le chiamate internazionali con CLI mobile, destinate a numeri fissi, a uno o più operatori mobili con cui ha stipulato degli accordi, utilizzando dei fasci specializzati. Gli operatori mobili agirebbero da operatori di transito per questo tipo di traffico e si occuperebbe di verificare se il CLI corrisponde al numero di un utente mobile in roaming, eventualmente interrogando le reti degli altri operatori mobili. Gli operatori mobili sarebbero remunerati per il transito.

Le chiamate con CLI mobile destinate a numeri mobili sarebbero inviate all'operatore mobile *recipient*.

Omissis ritiene che con questa soluzione gli operatori mobili dovrebbero occuparsi della gestione di un traffico che non gli compete e che questo possa essere accettabile solo nell'ottica di fornitura di un servizio sulla base di un accordo, non di un obbligo di regolamentazione. Gli operatori possono liberamente accordarsi per implementare in un certo modo la misura prevista dalla regolamentazione ma l'accordo non può essere imposto.

Omissis individua, nella soluzione proposta da Omissis, la fornitura di uno specifico servizio utile ai Carrier internazionali, quello di verifica ai fini del blocco delle chiamate con CLI mobile. Ritiene che questo servizio, che costituisce una possibile modalità per implementare la misura, debba essere fornito indipendentemente dai servizi di transito, eventualmente da soggetti terzi e su base negoziale. In ogni caso il traffico di spoofing dovrà essere bloccato prima possibile. Viceversa, delegando il controllo all'operatore di destinazione comporterebbe un aumento del consumo di risorse in termini di link e capacità degli apparati.

Omissis, confermando l'allineamento con gli operatori di rete mobile per l'implementazione della soluzione tecnica proposta, evidenzia che gli operatori mobili italiani con interconnessioni dirette con l'estero dovranno gestire il blocco dello spoofing per le chiamate di cui gestiranno il transito, oltre a offrire le API per gli altri operatori di transito. Ipotizza inoltre che, una volta attuate le misure di blocco, i tentativi di spoofing si ridurranno notevolmente, riducendo nel tempo anche il volume di query necessarie.

Agcom prende atto delle posizioni espresse e comunica ai partecipanti alla riunione la possibilità di inviare dei contributi scritti, entro lunedì 7 aprile, che riportino le posizioni espresse e, eventualmente, ulteriori osservazioni.

Per quanto riguarda il blocco delle chiamate con CLI non mobile, l'Autorità prende atto della sostanziale convergenza delle posizioni sugli aspetti principali della soluzione proposta. Le integrazioni richieste da Omissis saranno discusse in uno specifico confronto tecnico fra gli operatori che dovrà tenersi nel breve allo scopo di giungere a una soluzione pienamente condivisa.

In merito al blocco delle chiamate con CLI mobile l'Autorità prende atto delle opinioni espresse.

La riunione termina alle ore 12:30.

Allegato

Elenco dei partecipanti

Assocall
Assoutenti
BT
CertFIN
Colt
Commify
Eolo
Fastweb
Fibercop
Iliad
Intermatica
MCLINK
Messagenet
NHM
OpenGate
Postepay
Sky
Sparkle
Studio Gallotto
TATA Communications
TIM
Udicon
Verizon
Vianova
Vodafone
WindTre

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Resoconto sintetico della riunione del tavolo tecnico del 3 aprile 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera n. 457/24/CONS

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui all'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Resoconto sintetico della riunione del 3 aprile 2025

Il giorno 3 aprile 2025, alle ore 16:00, si è tenuta in videoconferenza una riunione del tavolo tecnico convocato nell'ambito del procedimento avviato con la delibera n. 457/24/CONS. La seduta ha avuto l'obiettivo di discutere alcune proposte di integrazione, formulate dagli operatori Omissis e Omissis, riguardanti la soluzione tecnica discussa nella seduta del 27 marzo 2025, con specifico riferimento all'attuazione delle misure di cui al comma 1 e alle lettere a) e b) del comma 2 dell'articolo 8 dello schema di provvedimento sottoposto a consultazione pubblica.

L'incontro ha visto la partecipazione degli operatori Omissis, Omissis, Omissis, Omissis, Omissis, Omissis e Omissis e dei rappresentanti dell'Autorità.

Nella prima fase della riunione Omissis ha richiesto alcune modifiche di carattere formale alle slides che descrivono la proposta tecnica ed ha ribadito la non condivisione della soluzione tecnica proposta nel documento riepilogativo per la gestione delle chiamate con CLI mobile. In tale contesto l'operatore chiede che venga rimosso il riferimento alle linee guida GSMA - IR65 nelle tematiche inerenti al CLI della numerazione fissa.

Si è poi aperta un'ampia discussione sulle integrazioni richieste da Omissis con riferimento alla gestione delle chiamate internazionali con CLI di rete fissa, con tesi opposte circa il rapporto costi/benefici delle stesse.

Ad esito di tale discussione è stato raggiunto un accordo in merito:

- all'inserimento, fra i casi di blocco, delle chiamate con CLI di rete fissa che contiene solo il country code italiano seguito dalla cifra zero,
- a inserire fra le eccezioni al blocco le chiamate con CLI geografico dirette ad un numero internazionale ovvero non appartenente al Piano di Numerazione Italiano.

Non è stata invece raggiunta una posizione comune riguardo alla proposta di Omissis di bloccare le chiamate con CLI di rete fissa che contiene un country code inesistente o non assegnato e a quelle che presentano il country code nazionale seguite dal solo numero di distretto.

A tale riguardo, gli operatori Omissis, Omissis, Omissis, Omissis e Omissis si sono riservati di effettuare delle verifiche e di riportarne l'esito in una successiva seduta del tavolo.

Con riferimento alla reportistica, Omissis, Omissis, Omissis, Omissis e Omissis hanno realizzato una ipotesi sulle informazioni da raccogliere ed inviare; Omissis ha invece proposto che sia l'Autorità a determinare i dati oggetto di invio e le relative modalità.

Viene fissata una nuova riunione per mercoledì 9 aprile.

La riunione termina alle ore 18.30

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Resoconto sintetico della riunione del tavolo tecnico del 9 aprile 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera n. 457/24/CONS

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui all'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Resoconto sintetico della riunione del 09 aprile 2025

Il giorno 9 aprile 2025, alle ore 10:15, si è tenuta in videoconferenza una riunione del tavolo tecnico convocato nell'ambito del procedimento avviato con la delibera n. 457/24/CONS. La seduta ha avuto l'obiettivo di proseguire la discussione, avviata nella seduta del 3 aprile 2025, in merito ad alcune proposte di integrazione, formulate dagli operatori Omissis e Omissis, riguardanti la soluzione tecnica discussa nella seduta del 27 marzo 2025, con specifico riferimento all'attuazione delle misure di cui al comma 1 e alle lettere a) e b) del comma 2 dell'articolo 8 dello schema di provvedimento sottoposto a consultazione pubblica.

L'incontro ha visto la partecipazione degli operatori Omissis, Omissis, Omissis, Omissis, Omissis, Omissis e Omissis e dei rappresentanti dell'Autorità.

Omissis ha ribadito l'esigenza di apportare alcune modifiche di carattere formale alle slides che descrivono la soluzione in discussione e la mancata condivisione delle sezioni del documento che riguardano la parte definitoria e la soluzione tecnica per le chiamate con CLI mobile.

Si è poi passati a discutere le integrazioni proposte da Omissis che nella riunione del 3 aprile non erano state condivise dagli altri operatori, con l'eccezione di Omissis.

Omissis, Omissis, Omissis Omissis e Omissis hanno manifestato una posizione definitivamente contraria all'introduzione di un obbligo di blocco delle chiamate con country code inesistente o non assegnato e delle chiamate con country code nazionale seguito dal solo prefisso distrettuale. Gli stessi operatori ritengono che tali blocchi debbano al più essere considerati opzionali.

Si è aperta una discussione in proposito in cui sono state sostanzialmente ribadite le motivazioni delle due tesi. Omissis ha precisato che la sua proposta è volta a massimizzare le tutele, non manifestando un'assoluta contrarietà a una sua implementazione opzionale o comunque da effettuarsi in una fase successiva.

L'Autorità ha preso atto delle rispettive posizioni

La termina alle ore 11:30

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Resoconto sintetico della riunione del tavolo tecnico del 15 aprile 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera n. 457/24/CONS

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui all'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Resoconto sintetico della riunione del 15 aprile 2025

Il giorno 15 aprile 2025, alle ore 15:30, si è tenuta in videoconferenza una riunione del tavolo tecnico convocato nell'ambito del procedimento avviato con la delibera n. 457/24/CONS. La seduta ha avuto l'obiettivo di illustrare alcune integrazioni alla soluzione tecnica discussa nelle sedute del 27 marzo e del 1° aprile, introdotte dai proponenti in parte anche a seguito di successivi incontri con gli operatori Omissis e Omissis.

Le modifiche al documento interessano in particolare la casistica di blocco per CLI non mobile; la formulazione dei casi di blocco per CLI mobile; l'introduzione della reportistica relativa ai blocchi per CLI non mobile e della specifica tecnica delle API funzionali al blocco per CLI mobile nella soluzione in discussione.

L'incontro ha visto la partecipazione delle principali associazioni dei consumatori, associazioni di imprese, operatori di telecomunicazioni (TLC) e altri attori rilevanti, tra cui esperti e operatori di altri settori direttamente coinvolti nella questione del CLI spoofing, oltre che dei rappresentanti dell'Autorità.

L'elenco delle società partecipanti è riportato in allegato.

AGCOM, illustra le modifiche introdotte al documento invitando i presenti a esprimere eventuali commenti su ciascun punto.

Omissis in premessa manifesta di non condividere la definizione di Carrier Internazionale, non prevista dal Codice delle Comunicazioni, e gli obblighi di notifica previsti dalla proposta tecnica.

Con riferimento alla reportistica, **Omissis** osserva che quanto si propone di introdurre nell'ambito della proposta esula dal provvedimento dell'Autorità che non include obblighi di reportistica. L'operatore ritiene inoltre che i report proposti non sarebbero utili a valutare l'andamento del fenomeno di spoofing in quanto il numero di chiamate bloccate non rappresenterebbe un indicatore significativo.

A parere di **Omissis**, invece, la reportistica è utile a fornire indicazioni sull'attività di contrasto svolta. L'operatore ritiene che, per evitare un sovraccarico delle risorse di calcolo, i report debbano riguardare i contatori di rete e non i singoli eventi che possono invece essere estratti su richiesta. L'operatore ritiene che la struttura del report proposta nel documento sia adeguata.

Omissis concorda sull'utilità della reportistica.

Omissis ricorda che anche in relazione al blocco delle chiamate che non rispettano la Raccomandazione ITU-T E.164, richiesta nell'ambito dei lavori del Comitato Tecnico sulla Sicurezza nelle Comunicazioni, l'Autorità ha chiesto di produrre dei Report. Secondo l'operatore la reportistica è fondamentale per avere contezza di ciò che viene bloccato e per conoscere il

comportamento degli operatori esteri in relazione alla consegna di traffico affetto da spoofing. Informazione che potrà essere utile all'Autorità nelle attività che si svolgono in ambito europeo, anche per sensibilizzare gli altri paesi a introdurre norme sull'inalterabilità del CLI, attualmente presenti in pochissimi paesi europei.

Altra cosa sono poi le segnalazioni degli utenti che contribuiscono a monitorare il fenomeno e si riferiscono a chiamate che l'operatore non è in grado di classificare a priori come spoofing.

In merito alla casistica di blocco nel caso di CLI mobile, riportata alla slide 10 del documento che descrive la soluzione tecnica proposta, si apre un ampio dibattito relativo alla modalità tecnica per discriminare efficacemente le chiamate da bloccare.

A tale riguardo, **Omissis** mostra una tabella che evidenzia come i casi in cui la chiamata deve essere bloccata siano identificabili tecnicamente, in modo affidabile, dallo stato di registrazione in HLR del cliente che ha in uso il numero corrispondente al CLI. In particolare, le chiamate da bloccare sono quelle per le quali l'utente risulta registrato in Italia nel dominio 2G/3G o non risulta registrato affatto nel dominio 2G/3G.

Omissis si riserva di fare un'ulteriore verifica interna prima di confermare che, anche nella sua rete, la modalità di verifica dei casi di blocco possa limitarsi al controllo dello stato di registrazione in HLR.

Omissis chiede il motivo dell'esclusione, fra le eccezioni al blocco delle chiamate con CLI mobile, del caso di chiamate dirette a numeri internazionali, inserite invece come eccezioni per le chiamate con CLI fisso.

A seguito di una breve discussione i presenti concordano sull'opportunità di inserire tale eccezione; dunque, le chiamate con CLI mobile dirette ad un numero internazionale ovvero non appartenente al Piano di Numerazione Italiano non dovranno essere bloccate.

Omissis chiarisce che le due fasi indicate nel documento riguardanti il blocco delle chiamate con CLI mobile sono da intendersi come fasi operative nell'analisi delle chiamate e non fasi di implementazione. Nella prima fase il Carrier Internazionale effettua autonomamente le verifiche riguardanti lo stato di assegnazione delle numerazioni e il verificarsi delle eccezioni previste, operando i relativi blocchi se del caso.

Se nella prima fase si rileva che la chiamata non rientra fra le eccezioni previste e il CLI corrisponde a un numero assegnato a un operatore mobile, si passa alla seconda fase che prevede l'interrogazione dell'operatore mobile sulla cui rete è configurato il numero per mezzo delle API. Le funzionalità previste dalle due fasi saranno implementate assieme.

Omissis ricorda l'osservazione, manifestata anche nelle precedenti riunioni, circa il fatto che, se il blocco dei numeri non assegnati fosse implementato per primo, il fenomeno dello

spoofing potrebbe utilizzare numeri assegnati, con conseguente disturbo recato agli utenti assegnatari che verrebbero contattati dagli utenti che ricevono chiamate di spoofing.

Omissis e Omissis concordano con Omissis circa l'opportunità di procedere contestualmente all'implementazione delle funzionalità di fase 1 e fase 2 per evitare che lo spoofing si concentri sui numeri attivi.

Omissis è di parere opposto e, vista la diffusione dello spoofing basato sull'utilizzo delle numerazioni mobili, ritiene importante agire prima possibile, operando al più presto i blocchi più semplici da implementare.

Omissis richiama l'onerosità per gli operatori delle soluzioni di contrasto allo spoofing ed evidenzia che l'implementazione delle funzionalità previste nelle due fasi di blocco delle chiamate con CLI deve tener conto degli aspetti tecnici di sviluppo, in tal senso non risultano fattibili due implementazioni disgiunte.

Tornando alla soluzione proposta per il blocco delle chiamate internazionali con CLI mobile, su richiesta di **Omissis,** gli operatori mobili confermano che le chiamate in roaming effettuate esclusivamente su rete 4G non transitano per le interfacce internazionali.

Omissis osserva che, essendo un operatore di transito, non dovrebbe essere coinvolta in aspetti che non le competono come quello della verifica dello stato di roaming. Suggerisce di incentivare la dismissione delle tecnologie 2G/3G o comunque l'utilizzo del protocollo CAMEL.

Omissis ribadisce che la soluzione che si sta discutendo è inutilmente complessa essendo legata alla presenza di tecnologie (2G/3G) in fase di dismissione. L'operatore riporta inoltre che, in Belgio, i primi risultati della soluzione basata sul CAMEL appaiono positivi e chiede all'Autorità di valutare, anche tenendo conto dei "numeri", entrambe le soluzioni, quella basata sulle query e quella basata sull'utilizzo dell'HRN.

Omissis ribadisce la criticità connessa alla parziale diffusione degli accordi di roaming basati su CAMEL e all'inefficacia dell'anonimizzazione che si renderebbe necessaria per evitare il blocco di chiamate di utenti in roaming su reti estere che non utilizzano CAMEL.

Riguardo ai blocchi opzionali per le chiamate internazionali con CLI mobile, **Omissis** ritiene che debba essere chiarito che la logica di blocco non può basarsi su database forniti da terze parti, ma unicamente su valutazioni interne dell'operatore.

La riunione termina alle ore 18:05.

Allegato

Elenco dei partecipanti

A2A
Adiconsum
AIIP
Altroconsumo
Assocall
Assoutenti
BT
Colt
Commify
Coop
Edison
Elettricità Futura
Enel
Eolo
Fastweb
FiberCop
Hal Service
Iliad
Messagenet
OpenGate
Optima Italia
Postepay
Proxigas
Retelit
Sky
Sparkle
Studio Gallotto
Studio legale Dalla Vedova
Tim
Verizon
Vianova
Vodafone
WindTre

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Delibera 457/24/CONS

Resoconto sintetico della riunione del tavolo tecnico del 23 aprile 2025

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Direzione tutela dei consumatori

Delibera n. 457/24/CONS

Tavolo tecnico per la definizione delle modalità implementative delle misure tecniche di blocco di cui all'art. 8 dell'allegato B alla delibera n. 457/24/CONS

Resoconto sintetico della riunione del 23 aprile 2025

Il giorno 23 aprile 2025, alle ore 14:30, si è tenuta in videoconferenza una riunione del tavolo tecnico convocato nell'ambito del procedimento avviato con la delibera n. 457/24/CONS. La riunione ha avuto l'obiettivo di discutere una serie di tematiche anticipate nell'e-mail di convocazione:

- specifiche tecniche delle API previste dalla soluzione tecnica proposta per il blocco delle chiamate internazionali con CLI mobile;
- possibile variante della soluzione proposta per le chiamate con CLI mobile basata su un soggetto che opera da proxy e agisce da intermediario fra i carrier internazionali e gli operatori mobili;
- blocco delle chiamate con CLI corrispondente a SIM usate per servizi M2M;
- efficacia della soluzione proposta nel contrastare lo spoofing che fa uso di numeri "sensibili";
- necessità dell'accordo quadro proposto per la soluzione relativa al CLI mobile.

L'incontro ha visto la partecipazione delle principali associazioni dei consumatori, associazioni di imprese, operatori di telecomunicazioni (TLC) e altri attori rilevanti, tra cui esperti e operatori di altri settori direttamente coinvolti nella questione del CLI spoofing, oltre che dei rappresentanti dell'Autorità.

L'elenco delle società partecipanti è riportato in allegato.

Ad esito della riunione del 15 aprile **Omissis** si era riservata di verificare la possibilità di utilizzare unicamente le informazioni presenti in HLR per discriminare i casi di blocco delle chiamate internazionali con CLI mobile. L'operatore conferma tale modalità di verifica che risulta pertanto condivisa da tutti i partecipanti, ad eccezione di coloro che non condividono l'intera soluzione proposta per il blocco delle chiamate internazionali con CLI mobile.

Si apre una discussione in merito un'osservazione di **Omissis** relativa alla previsione, inclusa nella specifica delle API, secondo cui in caso di picchi di interrogazione che possano mettere in difficoltà l'integrità della rete, l'operatore mobile può limitare le risposte alle chiamate ricevute, inviando un messaggio di "non blocco".

A parere dell'associazione tale previsione può rappresentare una vulnerabilità del sistema, sfruttabile da soggetti malintenzionati che potrebbero provocare volontariamente un sovraccarico al fine di evitare i blocchi. È necessario dunque prevedere degli accorgimenti per preservare il più possibile la funzione di blocco: dimensionamento e scalabilità adeguati; ottimizzazione delle interrogazioni con meccanismi di caching; rate shaping e gestione dei picchi; soglie adattative e monitoraggio continuo. Inoltre, in caso di sovraccarico del sistema, è opportuno prevedere comunque il blocco delle chiamate. In tal modo si produrrebbe al più un ritardo per le chiamate

lecite che dovessero essere bloccate per il mancato controllo dello stato di roaming. Un utente in roaming che si vede la chiamata bloccata può infatti effettuare un nuovo tentativo successivamente.

Omissis condivide la necessità di adottare un approccio opportunamente prudenziale nel dimensionamento delle risorse. Osserva però che è sempre possibile il verificarsi di picchi che superano le soglie previste. In tal caso occorre privilegiare la continuità del servizio telefonico. È sempre possibile, poi, rivedere il dimensionamento delle risorse nel caso in cui se ne rilevasse l'esigenza.

Omissis ritiene inoltre che una strategia di blocco delle chiamate in caso di sovraccarico del sistema richiederebbe una base legale molto forte per tutelare gli operatori in caso di contestazioni, questi dovrebbero essere salvaguardati da qualsiasi rischio derivante da operazioni di blocco per le quali non sono in grado di verificare a priori la correttezza.

Omissis conferma che il dimensionamento previsto non è "statico" ma potrà essere modificato per adeguarlo a picchi di richieste inizialmente non previsti. L'operatore osserva inoltre che le connessioni di traffico internazionali hanno un dimensionamento abbastanza definito e basato sul traffico abituale; pertanto, tali connessioni mal si prestano a supportare picchi di traffico legati ad attacchi mirati.

Omissis condivide tali affermazioni aggiungendo che non è possibile adottare una logica che privilegi il blocco delle chiamate in caso di sovraccarico del sistema contando sul fatto che, nel caso di blocco di chiamate lecite, l'utente possa richiamare. L'operatore osserva in proposito che determinate chiamate di utenti in roaming all'estero possono rivestire un'importanza molto elevata, riguardando ad esempio utenti in difficoltà, magari non in grado di rivolgersi altrove e impossibilitati ad effettuare un ulteriore tentativo di chiamata.

Omissis e Omissis ritengono opportuno introdurre un *rating* per le società che dimostreranno la loro accountability sul tema dello spoofing, in modo da evidenziare i più virtuosi.

Omissis chiede agli operatori che hanno proposto la soluzione tecnica di chiarire il rapporto fra l'accordo quadro, previsto per formalizzare il processo di interazione fra carrier internazionali e operatori mobili, e gli accordi bilaterali indicati nella descrizione delle API in relazione allo stabilimento di connessioni sicure fra tali soggetti.

Secondo l'operatore, per ragioni di efficienza e di riduzione delle tempistiche, è opportuno dettagliare i processi nell'ambito del provvedimento piuttosto che demandare tale attività alla fase di stipula di un accordo quadro.

Omissis ritiene che l'accordo quadro sia necessario ad armonizzare il più possibile le implementazioni di tutti gli operatori. Tuttavia, la messa in opera del sistema richiede poi anche una fase di test. Saranno dunque necessari degli accordi bilaterali per definire puntualmente la messa in esercizio delle query di blocco delle chiamate con CLI mobile.

L'operatore ritiene che alcuni aspetti, quali quello dell'assurance, non possano essere definiti efficacemente in una delibera, considera opportuno prevedere un accordo quadro "snello" e minimizzare gli accordi bilaterali, limitandoli eventualmente ai soli aspetti implementativi.

Omissis, consapevole dell'esigenza di stabilire processi di esercizio e assurance uniformi per tutti gli operatori, ritiene preferibile che questi siano definiti da linee guida pubblicate da Agcom o dal Ministero piuttosto che da un accordo quadro. Nel corso della definizione di quest'ultimo potrebbero infatti sorgere posizioni inconciliabili da parte dei diversi operatori che richiederebbero comunque un intervento dell'Autorità.

Omissis chiede di chiarire se l'azione di armonizzazione fra i campi "PAI" e "From", riportata nella slide n. 5 del documento che descrive la soluzione (si fa riferimento alla versione diffusa prima della riunione), debba essere attuata dal carrier internazionale come azione preliminare solo nel caso di chiamate internazionali con CLI non mobile o anche nel caso di chiamate con CLI mobile.

Omissis chiarisce che, nell'intenzione dei proponenti, l'azione di armonizzazione è preliminare a entrambi i tipi di blocco e afferma che, se occorre, il documento può essere modificato per descrivere meglio tale aspetto.

Omissis osserva che secondo quanto previsto dalla soluzione proposta**,** ciascun carrier dovrà gestire un'interfaccia verso ciascun operatore mobile e viceversa, con una conseguente complessità in termini di procedure di esercizio e anche un certo dispendio di indirizzi IP pubblici che costituiscono una risorsa scarsa. A tal proposito Omissis non esclude la possibilità di affidarsi ad un eventuale operatore che decidesse di operare come hub per accorpare le query provenienti da più soggetti.

Omissis ritiene che una soluzione basata su un soggetto che agisce da hub centralizzato presenti una serie di svantaggi riguardanti la necessità di individuare un soggetto *trusted*, che necessariamente non può essere un operatore, l'allungamento dei tempi di setup delle chiamate e la necessità di remunerare chi opera da hub.

Omissis ritiene che alcuni operatori possano anche accordarsi per via commerciale, delegando un operatore ad agire da hub. Concorda con Omissis in merito agli svantaggi di una soluzione complessivamente basata su hub.

In merito all'inserimento, fra i casi di blocco, dei numeri usati per servizi M2M, **Omissis** osserva che gli operatori non sono in grado di discriminare tale utilizzo e che alcuni servizi di questo tipo prevedono la generazione di chiamate vocali, come nel caso delle eCall.

Riguardo alla tutela legata a numeri "sensibili" (quali quelli di banche, polizia ecc.) **Omissis e Omissis** chiariscono che la soluzione proposta, prevedendo il blocco delle chiamate internazionali con CLI corrispondente delle numerazioni geografiche e non geografiche diverse dai numeri mobili, risulta efficace allo stesso modo per tutte le numerazioni, incluse quelle "sensibili".

L'Autorità chiede agli operatori che hanno proposto la soluzione tecnica di chiarire l'esigenza, da loro manifestata, di poter generare i cartellini di traffico per le chiamate bloccate.

In proposito, **Omissis** rappresenta che le norme previste dal Garante della Privacy prevedono che le informazioni relative alle chiamate che non raggiungono l'utente possano essere mantenute per un tempo molto breve. Successivamente devono essere archiviate e possono essere rese disponibili solo nell'ambito delle prestazioni obbligatorie per fini giudiziari. Tale impianto, applicato alle chiamate bloccate, non consentirebbe di effettuare approfondimenti per gestire

richieste di spiegazione da parte di operatori che si vedono bloccate le chiamate consegnate al carrier internazionale.

Avendo esaurito le tematiche in discussione e constatata l'assenza di altre osservazioni, l'**Autorità** ringrazia i presenti e dichiara conclusa la fase del tavolo tecnico dedicata alle misure per il blocco delle chiamate internazionali.

La riunione termina alle ore 15:45.

Allegato

Elenco dei partecipanti

A2A
Altroconsumo
AssoCall
Assoutenti
BT
Codacons
Colt
Commify
Coop
Edison
Elettricità Futura
Engie
Fastweb
Fibercop
Hal Service
Iliad
MessageNet
MyWic
Octopus Energy
OpenGate
Postepay
Proxigas
Retelit
Sky
Studio Gallotto
Studio legale Dalla Vedova
Tata Communications
Tim
Vianova
Vodafone
WindTre