AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Allegato 1 alla delibera n. 86/21/CIR

Esiti della consultazione pubblica inerente alla delibera n. 334/20/CIR concernente "Avvio di un procedimento e di una consultazione pubblica sulla integrazione delle procedure di portabilità del numero mobile, di cui alla delibera n. 147/11/CIR, e sulle connesse misure finalizzate ad aumentare la sicurezza nei casi di sostituzione della SIM (SIM Swap)"

1. Il procedimento

Hanno risposto alla consultazione 9 fornitori di servizi di comunicazione elettronica: Coop Italia Società Cooperativa, Fastweb S.p.A., Iliad Italia S.p.A., Kaleyra S.p.A., Postepay S.p.A., Telecom Italia S.p.A., Vodafone Italia S.p.A., Welcome Italia S.p.A., Wind Tre S.p.A. e tre associazioni dei consumatori: Coordinamento di associazioni per la tutela dell''ambiente e dei diritti di utenti e Consumatori (Codacons), Federconsumatori e Osservatorio Imprese e Consumatori (OIC).

Sono state tenute le audizioni individuali con le società Iliad Italia S.p.A., Wind Tre S.p.A. e Kaleyra S.p.A., su richiesta delle medesime società pervenute nei termini previsti, in data 28 gennaio 2021 (Iliad e Wind Tre) e il 29 gennaio 2021 (Kaleyra).

2. Sintesi dei contributi ricevuti dai soggetti rispondenti alla consultazione e valutazioni dell'Autorità

Di seguito si rappresentano sinteticamente, per ogni tema posto a consultazione, le risposte e le osservazioni dei soggetti rispondenti conferenti con l'oggetto del procedimento. In relazione ai riferimenti di alcuni rispondenti a quanto in corso nell'ambito del Comitato Tecnico Antifrode (CTA), istituito con la delibera n. 418/07/CONS, si evidenzia che tale attività è da ritenersi parallela a quella della presente consultazione che ha fini regolamentari. Per cui tali questioni esulano dall'ambito di applicazione del presente procedimento.

Testo in consultazione relativamente al criterio n. 1

"*Estensione a tutti i casi di cambio SIM dell'obbligo di identificazione del soggetto a cui viene data in uso una SIM (fisica o tramite caricamento via etere del profilo su eSIM) sia presso il dealer sia in caso di richiesta per via telematica, attuando le vigenti norme in tema di identificazione. Ciò è dovuto al fatto che in alcuni casi di cambio SIM potrebbero non essere attualmente adottate le medesime procedure e ciò potrebbe costituire una possibile debolezza del sistema in termini di sicurezza*."

Sintesi delle osservazioni del mercato sul criterio n. 1

Nessun rispondente si dichiara contrario alla proposta. La quasi totalità dei rispondenti si esprime a favore di tale estensione, riconoscendo che l'assenza di tale obbligo di identificazione in alcune fattispecie può essere causa di un incremento di cambi SIM non voluti. Solo due rispondenti ritengono che le misure dagli stessi adottate siano già adeguate, senza esprimersi esplicitamente riguardo alla proposta di estensione.

Un rispondente rappresenta di operare già in tal senso. Alcuni rispondenti ritengono che i cambi SIM devono essere effettuati esclusivamente dal titolare della SIM. Uno dei rispondenti ritiene che quanto prospettato debba essere valido solo nel caso di SIM dedicate ai contratti *consumer*. Uno di questi rispondenti, limitatamente al caso del cambio SIM senza cambio operatore, ritiene che questo debba essere previsto se richiesto esclusivamente dal titolare del contratto, eventualmente tramite delega. Due rispondenti ritengono che la gestione di casi di MNP richiesta dal reale utilizzatore non abbia evidenziato negli anni criticità rilevanti. Alcuni rispondenti fanno riferimento anche all'utilità dell'uso della delega, escludendo il caso di furto o smarrimento. Uno dei rispondenti rappresenta di non accettare autodichiarazioni anche laddove normalmente consentite dalla legge.

Alcuni rispondenti ritengono che le modalità di identificazione debbano essere diverse nel caso dei contratti *consumer* e *business*. Un rispondente ritiene che sia fondamentale che sia lasciata autonomia operativa e commerciale agli operatori sulle modalità di identificazione, purché queste siano tali da garantire il rispetto della normativa di settore in materia, al fine di evitare interventi onerosi ed invasivi sui processi e sistemi informativi degli operatori. Tali aspetti sono considerati con riferimento al criterio n. 2.

Valutazioni dell'Autorità relativamente al criterio n. 1

Anche in considerazione del fatto che la quasi totalità dei rispondenti si è espressa a favore, l'Autorità ritiene di confermare il principio sottoposto a consultazione specificando che le richieste di sostituzione SIM possono essere effettuate solo dal titolare della SIM, ad eccezione dei casi di SIM aziendali laddove siano fornite all'azienda riserve di SIM gestite dall'azienda stessa.

L'uso della delega può essere consentito, esclusivamente, qualora siano attuati metodi aggiuntivi di verifica: esplicito assenso via SMS al numero principale o chiamata registrata effettuata dall'operatore mobile verso il numero principale, mentre non si ritiene applicabile la possibilità che la chiamata provenga dal numero principale del cliente, per evitare cambi indesiderati a seguito di *spoofing* del CLI. Maggiori dettagli sono forniti relativamente agli altri criteri.

Di conseguenza, in caso di SIM guasta, smarrita o rubata, la delega non è consentita e il cambio è effettuato dal titolare.

Nel caso di furto deve essere presentata relativa denuncia alle autorità competenti e acquisito l'originale dal punto vendita.

L'Autorità non ritiene accoglibile la richiesta di mantenere la previsione attuale, secondo cui un soggetto terzo che si auto dichiara reale utilizzatore, possa richiedere la MNP, ciò in quanto si sono verificati casi di MNP effettuate da soggetti che non erano i rispettivi titolari e sono state contestate.

Gli operatori potranno prevedere il cambio di titolare del contratto senza cambio SIM (subentro) con l'utilizzo di opportuni sistemi di sicurezza, compreso l'assenso esplicito via SMS o via OTP.

Nell'atto di consegna ad una azienda deve essere identificato il soggetto delegato dall'azienda a ritirare le SIM. Non rientra, quindi, nell'eccezione il caso di singole SIM *business* associate a partita IVA, laddove non sia previsto la fornitura di SIM di riserva gestite dall'azienda.

L'Autorità ritiene, infatti, che nel caso di fornitura di varie SIM ad un'azienda, gestite dalla stessa anche tramite l'ausilio dell'operatore, sia giustificato che le SIM siano date ai responsabili preposti dell'azienda e non ai singoli utenti utilizzatori delle stesse, fermo restando quanto previsto dalle norme di legge.

Le modalità minime di identificazione nel caso di fornitura di SIM come riserva fredda e, pertanto, senza identificazione immediata dell'utilizzatore sono definite dal Tavolo tecnico.

Testo in consultazione relativamente al criterio n. 2

"In tutti i casi di sostituzione della SIM, il fornitore di servizi mobili deve verificare, mediante identificazione, che il richiedente sia il titolare del contratto. In particolare:

- *nel caso in cui il cliente si rivolga, per la sostituzione della SIM, al proprio operatore, il dealer dovrà richiedere al cliente un documento di identità e la vecchia SIM (e trattenerla nel caso di immediata attivazione della nuova; a quanto noto, infatti, in questa fase si sono verificate frodi mediante falsificazione dei documenti o per mancata esibizione degli stessi, come sopra riportato al punto 1);*
- *nel caso in cui il cliente si rivolga per la sostituzione della SIM ad altro operatore, fermo restando che il cliente deve essere identificato ai fini del nuovo contratto e dovrebbe essere regolamentato l'obbligo di effettuare fotocopia della vecchia SIM, operazione abitualmente posta in essere, occorrerà valutare gli opportuni adeguamenti nell'ambito delle procedure per la portabilità del numero mobile per ridurre la probabilità di sostituzione non autorizzate di SIM richieste da soggetti diversi dal reale contraente (per errore o in caso di frode). Infatti, sulla base delle attuali procedure di MNP il rigetto della richiesta di passaggio si basa semplicemente o sulla verifica della correttezza dell'associazione del numero telefonico con il Codice Fiscale (casi di abbonamento) o con il numero seriale della SIM (casi di traffico prepagato). Un primo esempio di frode potrebbe essere quello messo in opera da un soggetto che richieda il passaggio di un numero di un altro cliente, comunicando il corretto numero seriale della vecchia SIM o il Codice Fiscale, appartenenti al suddetto legittimo cliente intestatario e di cui, il malintenzionato, è venuto a conoscenza. In tal caso la procedura di passaggio può andare a buon fine e va a riguardare un altro cliente che, per l'effetto, perde il numero. Al fine di rafforzare la sicurezza del processo, si ritiene necessario che tutti i dealer effettuino i necessari controlli sui documenti, ma anche che il rigetto della richiesta di MNP si basi, nell'ambito della procedura regolamentata, sulla verifica* ***sia del Codice Fiscale sia del numero seriale della SIM*** *considerando più complesso che vengano forniti entrambi corretti (anche grazie alla previsione di cui al punto 5);*
- *i due parametri (Codice Fiscale e numero seriale della SIM) sono già presenti nel sistema MNP e l'obbligo di presentazione, al dealer, di entrambi rafforzerebbe il controllo che, sulla base delle segnalazioni ricevute, se basato sul solo numero seriale della SIM si è rilevato insufficiente. Parimenti, l'utilizzo del solo Codice Fiscale risulta inadeguato in quanto facilmente individuabile da possibili frodatori. Pertanto, si ritiene che l'obbligo di presentare al dealer entrambi i dati possa incrementare la sicurezza del processo.*
- *Il principio di cui sopra si applica, in particolare, nel caso di SIM smarrita o rubata laddove il cliente si rivolga, per la sostituzione, a un nuovo operatore richiedendo la MNP. Le attuali procedure di MNP non prevedono alcun controllo in caso di smarrimento della SIM. In tal caso potrebbe verificarsi un errore di portabilità laddove venga digitato, al momento di inserimento dell'ordine, un*

numero telefonico errato. Fermo restando l'obbligo di identificazione ai fini del contratto, in questo caso il cliente dovrà esibire, oltre alla denuncia, un documento con il Codice Fiscale. In tal caso la procedura di MNP dovrebbe sempre prevedere la verifica del Codice Fiscale (anche nel caso di traffico prepagato);

- *In definitiva, sia nel caso in cui il cliente si rivolga al dealer del proprio operatore sia che richieda la MNP presso altro dealer, il dealer dovrà effettuare una copia di un documento d'identità del soggetto richiedente, di un documento attestante il Codice Fiscale, nonché della SIM o, eventualmente, della denuncia alle autorità competenti di smarrimento o furto della stessa. Per richieste per via telematica, oltre all'identificazione, come previsto dalle norme vigenti, dovrà essere previsto l'invio anche della copia della medesima documentazione richiesta in caso in cui ci si rivolga al dealer. La procedura di inserimento dati dovrebbe garantire, comunque, l'impossibilità di finalizzare la stessa se non vengono caricati a sistema la scansione dei documenti citati."*

Sintesi delle osservazioni del mercato sul criterio n. 2

Alcuni rispondenti concordano con le previsioni messe a consultazione, tra cui l'obbligo di effettuare una copia di un documento d'identità del soggetto richiedente, di un documento attestante il Codice Fiscale, nonché della SIM e, eventualmente, della denuncia alle autorità competenti di smarrimento o furto della stessa.

Un altro rispondente ritiene che le misure proposte non appaiano totalmente idonee ad aumentare il livello di sicurezza e siano non proporzionate esprimendo alcune motivazioni tra cui: la sperimentazione in corso nell'ambito del CTA, le misure proposte al punto 3) che include l'ipotesi di invio di una OTP, il fatto che il Codice Fiscale sia un documento con informazioni facilmente reperibili da parte dei possibili frodatori, degli sviluppi tecnici conseguenti, del fatto che in caso di sostituzione della SIM presso un *dealer* la vecchia SIM diverrebbe inutilizzabile.

In tema di "*Clienti consumer e business*"

Tre rispondenti ritengono che occorra distinguere il caso dei clienti *consumer* da quelli *business*.

Un rispondente analizza vari scenari e, in sintesi, mentre concorda che nel caso di MNP per contratti *consumer*, che rimangono tali, possa essere utile introdurre il doppio controllo (Codice Fiscale e ICC-ID), per gli altri casi ritiene che sia opportuna una valutazione in un Tavolo tecnico.

Con riferimento alla clientela *business*, un rispondente, a titolo di esempio, rappresenta di richiedere all'azienda Cliente di fornire, tra gli altri documenti, visura camerale e documento di identità del legale rappresentante.

In tema di "*Copia del documento d'identità*"

Un rispondente concorda sull'acquisizione della copia di un documento di identità del titolare dell'utenza.

Un altro rispondente ritiene che ai clienti *consumer* dovrebbe essere chiesto di esibire un documento di riconoscimento (oppure delega e copia del documento di riconoscimento del delegante) e di comunicare il Codice Fiscale. Specifica che nel caso di furto o smarrimento, la delega non è ammessa e deve presentare la relativa denuncia.

Altri due rispondenti concordano sulla copia del documento d'identità del richiedente.

Un altro rispondente ritiene che l'identificazione del cliente debba essere eseguita prima dell'attivazione della SIM, la quale potrebbe essere consegnata al cliente non attiva prima del completamento dell'identificazione e della messa a disposizione di un documento valido.

In tema di "*Copia del codice fiscale e all'occorrenza della denuncia*"

Un rispondente non concorda sull'obbligo dell'acquisizione e della conservazione delle copie del Codice Fiscale, della SIM o della denuncia alle autorità di pubblica sicurezza, ritenendo che, in tali casi, ci siano costi ed oneri eccessivi e non proporzionati. Tale rispondente ritiene che, generalmente, una tale procedura sia prevista dagli operatori solo in caso di portabilità e di sostituzione di SIM post-pagata presso la rete di vendita fisica. Lo stesso rispondente suggerisce alternative da valutare, quali criteri di verifica dell'identità dell'utente attraverso, ad esempio, l'elencazione delle ultime chiamate.

Al contrario un altro rispondente ritiene che il *dealer* debba effettuare una copia del documento attestante il Codice Fiscale, nonché della SIM o, eventualmente, della denuncia alle autorità competenti di smarrimento o furto della stessa. Inoltre, per richieste per via telematica, oltre all'identificazione, come previsto dalle norme vigenti, secondo tale rispondente dovrà essere previsto l'invio o il caricamento anche della copia della medesima documentazione richiesta in caso in cui ci si rivolga al *dealer*.

In tema di "*Ritiro e/o copia della SIM*"

Due rispondenti non concordano sull'opportunità di procedere al ritiro della vecchia SIM, rappresentando alcune motivazioni: *i*) non sarebbe possibile in tutti i casi; *ii*) in caso di uso di SMS (anche con OTP), è preferibile evitare complessità quali la consegna della SIM successivamente alla ricezione del messaggio; *iii*) ciò impedirebbe la gestione online dei processi, richiedendo la verifica della vecchia SIM spedita dal cliente; *iv*) il ritiro della vecchia SIM è un processo impegnativo dal punto di vista pratico in quanto, dovendo anche prevedere la verifica dell'ICC-ID stampigliato, si scontra con difficoltà dovute all'illeggibilità dello stesso (tipicamente per consunzione, almeno di qualcuna delle 19 cifre); *v*) il trattenere la vecchia SIM da parte del *dealer* può causare un disservizio al

cliente in quanto l'attivazione della nuova SIM generalmente non avviene in tempo reale e, pertanto, non sarebbe possibile garantire la continuità del servizio come avviene attualmente.

Un altro rispondente riferisce di chiedere al cliente la consegna della SIM in suo possesso.

Uno dei due rispondenti ritiene sproporzionato imporre l'obbligo di raccogliere una copia della vecchia SIM, in quanto onere notevole che rende il processo inefficiente e spesso pesante anche per il cliente finale, che dovrebbe estrarre la carta proprio nel momento della richiesta della MNP. Tale rispondente aggiunge che le procedure gestite dal canale online dovrebbero conseguentemente prevedere una ulteriore fase di scansione, upload e verifica della foto della SIM (oltre alle attuali di video-identificazione, e di foto e verifica del documento di identità), al punto di rischiare seriamente di non renderle più praticabili. L'altro rispondente ritiene, al contrario, che il *dealer* dovrebbe procedere alla visualizzazione della vecchia SIM ed effettuare obbligatoriamente la copia fotostatica della stessa. Tale rispondente ritiene che, nel caso di MNP, dovrebbe essere resa obbligatoria l'attuale prassi di effettuare una fotocopia della vecchia SIM.

Un altro rispondente ritiene che non sia necessario trattenere la vecchia SIM in quanto non è possibile garantire che la nuova SIM sia attiva immediatamente. Trattenere la SIM introdurrebbe significative complessità per richieste di sostituzione da remoto. Inoltre, tale rispondente ritiene che l'obbligo di effettuare una fotocopia della vecchia SIM non sia necessario, in quanto renderebbe ancor più complesso il processo di pre-validazione attualmente previsto dall'accordo quadro e in caso di eSIM non sarebbe possibile.

In tema di "*Doppio controllo (Codice Fiscale e ICC-ID)*"

Un rispondente ritiene che, nella MNP, nel caso di contratti *consumer* che rimangono tali possa essere utile introdurre il doppio controllo (Codice Fiscale e ICC-ID).

Anche un altro rispondente concorda sul fatto che il doppio controllo di Codice Fiscale e ICC-ID irrobustirebbe i processi di portabilità del numero, in particolare, nei casi di contratto post-pagato.

Un altro rispondente ritiene che prevedere la verifica sia del Codice Fiscale sia del numero seriale della SIM non permetterebbe di "rafforzare la sicurezza del processo" in quanto il *recipient* non è a conoscenza della titolarità della linea, oggetto di MNP.

Due rispondenti ritengono che la gestione di casi di MNP, richiesta dal reale utilizzatore, non abbia evidenziato negli anni criticità rilevanti. Uno dei due rispondenti aggiunge che i casi di frode riscontrati sono pressoché nulli. Pertanto, suggerisce di non introdurre per tutti i casi di MNP, una verifica congiunta del C.F. e del numero seriale della SIM.

Un altro rispondente ritiene che, pur essendo di per sé una misura apparentemente efficace per evitare richieste di portabilità di tipo fraudolento, tale previsione avrebbe un impatto sulla configurazione delle SIM di tipo pre-pagato in quanto, attualmente, le SIM possono essere utilizzate non direttamente dall'intestatario, ma dal cosiddetto Reale Utilizzatore (ad es. un congiunto). In questi casi, prima di poter presentare un'eventuale richiesta di

MNP, sarebbe necessario operare una sorta di subentro presso il proprio operatore al fine di far coincidere l'intestatario della SIM con colui che richiede effettivamente la portabilità. Ciò complicherebbe notevolmente le procedure di MNP, rischiando di veder aumentare i casi di KO in fase di validazione delle richieste.

In tema di "*Furto o smarrimento della SIM*"

Alcuni rispondenti propongono che, in caso di furto o smarrimento della SIM, il cliente, prima di effettuare la MNP, si debba rivolgere all'attuale operatore per avere una nuova SIM. Ciò corrisponde a vietare al *recipient* di accettare richieste di portabilità in caso di furto o smarrimento.

Un rispondente ritiene che sia opportuno uniformare l'obbligo di presentazione da parte del cliente all'operatore, prevedendo la medesima documentazione per il caso di furto e smarrimento. In particolare, ai fini della sostituzione della SIM, dovrebbe essere sempre presentata copia della denuncia fatta all'Autorità competente, sia in caso di furto che di smarrimento.

In tema di "*Nuova procedura con uso di OTP*"

Un rispondente chiede, altresì, che nell'ambito della presente consultazione sia integrato l'attuale processo di pre-validazione o validazione parziale con soluzioni opzionali che consistono nell'invio da parte del *recipient* di una OTP sulla SIM del *donating* per la quale il cliente intende richiedere la MNP. Ricevuto questa OTP via SMS al numero principale, il cliente restituirà al *recipient* l'OTP ricevuto via *web*. Il *recipient* potrà procedere con la richiesta di MNP senza trasmettere l'ICC-ID verso il *donating* e senza richiedere l'ICC-ID al cliente in quanto sostituito dalla OTP ricevuta sulla SIM oggetto di MNP. Il *recipient* potrà procedere solo dopo aver inserito nei propri sistemi tale OTP. Tale processo, in sostanza, sostituirebbe il processo di pre-validazione/validazione parziale e non necessiterebbe dell'uso, per la validazione, del numero seriale della SIM. In particolare, nella procedura telematica il cliente anziché inserire le informazioni relative a numero telefonico e all'ICC-ID della SIM dell'operatore di provenienza, inserirà le informazioni relative al numero di cellulare che intende portare, l'operatore di provenienza e una OTP (che il cliente riceverà sul numero che intende portare).

In tema di "*Flessibilità nell'uso dei canali di vendita e uniformità di comportamento*"

Un rispondente chiede che venga sempre concessa la possibilità alle imprese di scegliere i canali con i quali gli utenti possano richiedere una sostituzione della SIM e la MNP (presso i punti vendita, per via telematica).

Anche un altro rispondente ritiene che le stesse misure dovrebbero essere applicate per tutti i canali di vendita ed evitare differenziazioni per alcuni canali di vendita o per alcune casistiche, quali, ad esempio, il ritiro della vecchia SIM del cliente.

Valutazioni dell'Autorità relativamente al criterio n. 2

Clienti *consumer* e *business*

L'Autorità concorda con la richiesta per la quale alcuni clienti *business* possono avere trattamenti di identificazione diversificati in quanto possono avere specifiche esigenze, in particolare, nel caso di fornitura di riserve fredde, ovvero quando sono fornite SIM non attive per le quali non è noto il dipendente utilizzatore. Pertanto, per la clientela *business* si valuterà, in un apposito Tavolo tecnico, il caso di specie, nel rispetto delle norme vigenti in tema di identificazione dell'utilizzatore.

Copia del documento d'identità

Rilevato, altresì, che non sono state evidenziate contrarietà, l'Autorità conferma l'obbligo di effettuare copia del documento d'identità presentato in originale dall'intestatario, salvo deleghe limitatamente ai casi in cui è consentito sulla base della presente delibera. In merito alla richiesta per cui la SIM potrebbe essere consegnata non attiva al cliente prima del completamento dell'identificazione e della messa a disposizione di un documento valido, si ricorda che il Codice, art. 55, comma 7, prevede che "Ogni impresa è tenuta a rendere disponibili, anche per via telematica, al centro di elaborazione dati del Ministero dell'interno gli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile, che sono identificati prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica (S.I.M.)".

Copia del Codice Fiscale e all'occorrenza della denuncia

Per quanto concerne il Codice Fiscale, l'Autorità ritiene che dovrebbe essere sempre prevista copia del documento attestante lo stesso Codice Fiscale (tessera sanitaria) sia che il cliente si rivolga ad un *dealer* sia nel caso di richiesta autonoma da parte del cliente, ovvero tramite totem o per via telematica.

Nel caso di furto della SIM, l'Autorità ritiene che debba essere acquisita dal *dealer* l'originale della denuncia di furto, mentre nel caso di richiesta autonoma da parte del cliente, ovvero tramite totem o per via telematica, debba essere prevista l'acquisizione di copia della stessa.

Nel caso di smarrimento della SIM, l'Autorità ritiene che debba essere acquisita la relativa denuncia.

Nel caso di SIM guasta, considerato che non è prevista denuncia, l'Autorità ritiene che debba essere ritirata la vecchia SIM.

Ritiro e/o copia della SIM

L'Autorità, anche tenuto conto che nei casi di richiesta telematica è oneroso procedere a ritirare la SIM, ritiene che non debba essere obbligatorio effettuare il ritiro della SIM, ma solo la copia, e che salvo i casi di SIM guasta, smarrita o rubata, si dovrà prevedere una procedura con uno scambio SMS o fornitura di una OTP.

Doppio controllo (Codice Fiscale e ICC-ID)

Tenuto conto che l'Autorità per la MNP ritiene necessario uno scambio SMS o la fornitura di una OTP, si ritiene che non sia necessario il controllo dell'ICC-ID, mentre si conferma, per maggior sicurezza, che il Codice Fiscale dovrà essere sempre essere acquisito e trasmesso con la richiesta di MNP. L'Autorità ritiene di accogliere il suggerimento per cui lo scambio di un SMS o la fornitura di una OTP costituisca la validazione e, in tal caso, non sia necessario inserire tra i dati per la MNP l'ICC-ID.

L'Autorità intende rafforzare la sicurezza e ritiene che sia sempre necessario inserire il Codice Fiscale al fine di contrastare casi di MNP non voluti dall'intestatario e, pertanto, è opportuno che la richiesta debba essere effettuata dall'intestatario, salvo deleghe, laddove previste.

L'Autorità ritiene che debba essere oggetto di modifica la regola che consente al reale utilizzatore di effettuare la MNP e, pertanto, in questo caso dovrà essere cambiato preventivamente il nominativo del titolare (subentro), con tutte le cautele del caso.

Furto o smarrimento della SIM

L'Autorità concorda che, in caso di MNP, si debba escludere che il *recipient* possa accettare richieste di portabilità in presenza di SIM rubata o smarrita e, di conseguenza, il cliente debba rivolgersi, prima di procedere con la richiesta della MNP, all'attuale proprio operatore per richiedere una nuova SIM.

L'Autorità ritiene, altresì, che anche nel caso di SIM guasta il cliente debba essere invitato a rivolgersi, prima di procedere con la richiesta della MNP, all'attuale proprio operatore per ottenere una nuova SIM. Ciò, come chiarito nel seguito, al fine di evitare di dover prevedere tempi lunghi di attesa. Il caso di SIM guasta è trattata dall'attuale operatore in analogia al caso di SIM smarrita.

Flessibilità nell'uso dei canali di vendita e uniformità di comportamento

L'Autorità concorda in generale con la proposta e ritiene che le condizioni minime debbano valere per tutti i canali.

Portabilità indesiderata

In caso di portabilità indesiderata, in presenza di denuncia alla competente Autorità, è opportuno che il *recipient* e il *donating* realizzano rapidamente la portabilità inversa ripristinando la SIM e le condizioni contrattuali precedenti. I dettagli operativi e procedurali potranno essere determinati in apposito tavolo di lavoro.

Testo in consultazione relativamente al criterio n. 3

"In tutti i casi di sostituzione della SIM, il fornitore di servizi mobili invia sempre un messaggio SMS per informare il cliente che è stata richiesta la sostituzione della SIM e gli chiede conferma (a esempio mediante inserimento di una OTP) al fine di proseguire con le ulteriori procedure necessarie per esaudire la richiesta. In assenza di conferma esplicita, cosa che si verifica nei casi di SIM smarrita, rubata o guasta, si introduce un principio di attesa di un adeguato tempo (per esempio 72 ore) nel corso del quale il cliente, per altra via (ad esempio tramite e-mail o fornitura di un altro numero cellulare all'operatore) potrà essere informato del cambio SIM e, nel caso di cambio all'insaputa dell'utente, bloccare il processo.

A tal fine ai numeri mobili "principali" sono associati altri numeri mobili ed e-mail, validati con opportuna procedura di test, a cui verranno inviate le informazioni relative al processo di sostituzione della SIM, eventualmente limitando l'invio della OTP al solo numero principale e fornendo informazioni del processo ai numeri ed e-mail associati. Eventuali variazioni dopo l'adesione al contratto dei numeri ed e-mail associati dovrà avvenire sempre adottando criteri di sicurezza basati su OTP.

Ciò premesso, quando il cliente riceve l'informazione che si sta procedendo con la sostituzione della SIM, deve sempre avere la possibilità di bloccare tale processo in modo semplice, anche solo inviando un SMS ad un numero prefissato, concordato tra tutti gli operatori mobili e l'Autorità, con codice "40", ovvero chiamando il customer care e svolgendo la procedura in autonomia o parlando con un operatore, nonché accedendo ad un'area riservata sul sito web dell'operatore;".

Sintesi delle osservazioni del mercato sul criterio n. 3

In tema di "*Introduzione di una procedura o basarsi esclusivamente su identificazione dell'utente o su messaggi informativi*"

Un rispondente conviene sull'opportunità di introdurre, oltre a rigorose procedure di identificazione del cliente e di raccolta documentale, appositi meccanismi di sicurezza dei processi di sostituzione. Il rispondente rappresenta che a seguito della segnalazione di alcuni casi di frode messi in atto mediante la indebita sostituzione della SIM, abbia proattivamente attivato processi, simili a quelli posti a consultazione, che si stanno rivelando - al momento – efficaci.

Due rispondenti ritengono sufficiente una corretta identificazione del cliente presso il *dealer*, sostenendo che questa sia già efficace e in grado di tutelare il cliente e che ciò sia dimostrato dalle esigue percentuali del numero di frodi per cambio SIM. Pertanto, ritengono non necessaria una conferma esplicita da parte del cliente, ovvero l'introduzione di una OTP, per procedere con il cambio SIM, né tanto meno lunghi periodi di attesa. Inoltre, uno di questi rispondenti rappresenta che non si può inviare un SMS al numero associato alla SIM quando il punto vendita ha già effettuato il ritiro della SIM o la SIM è danneggiata.

Anche un altro rispondente ritiene che la misura proposta in consultazione sia di difficile implementazione e non sembri dare sufficiente garanzia nel contrastare efficacemente eventuali frodi a danno dei clienti. Tale rispondente ritiene che la soluzione migliore da mettere in campo, per dare comunque maggiore protezione al cliente potenzialmente oggetto di una sostituzione fraudolenta della SIM, sia di avvisare il cliente con un SMS (di tipo informativo) che sta per avvenire la sostituzione della SIM su cui ha ricevuto l'SMS stesso. Il cliente dovrebbe, quindi, avere la possibilità di poter "reagire" prontamente per mezzo della misura posta in consultazione dall'Autorità e, quindi, inviando un SMS ad un numero prefissato, chiamando il *customer care*, accedendo ad un'area riservata sul sito *web* dell'operatore e svolgendo la procedura in autonomia o parlando con un operatore. Lo stesso rispondente ritiene che sia complesso e inefficace l'uso di numeri o e-mail addizionali e che l'utilizzo dell'SMS non sia uno strumento sicuro per veicolare la OTP e cita a, titolo di esempio, una frode subita da WhatsApp proprio sul sistema di OTP utilizzato per consentire di accedere alle chat, indicando che il frodatore sfrutta metodi di "*social engineering*".

Un altro rispondente ritiene che potrebbe essere prevista un'estensione ai casi di sostituzione della SIM dell'attuale meccanismo di pre-validazione, previsto per la MNP, previa convocazione di un apposito Tavolo tecnico e modifica dell'Accordo Quadro di MNP. Nello specifico caso di sostituzione di SIM smarrita o rubata, rivolgendosi all'attuale operatore, l'OTP dovrebbe essere inviata ad un contatto dell'utente alternativo a quello principale (SMS o e-mail) a scelta dell'operatore. In tal caso, dovrebbe essere prevista sempre una conferma esplicita da parte del cliente che riceve l'OTP sul contatto alternativo e, pertanto, il meccanismo di attesa non risulterebbe più necessario per proseguire con l'operazione.

Un altro rispondente rappresenta che la procedura adottata dallo stesso per la sostituzione della SIM in caso di furto e smarrimento prevede che *i*) il cliente presenti la denuncia di furto o smarrimento; *ii*) venga inviato un SMS di avviso al MSISDN associato alla SIM di cui si richiede la sostituzione; *iii*) la richiesta passa alla verifica del *back office* che analizza puntualmente:

- la corrispondenza dei documenti presenti a sistema con quelli presentati dal cliente;
- l'apparente non contraffazione dei documenti;
- la coerenza del luogo di richiesta con il luogo di attivazione;
- l'attendibilità formale della denuncia di smarrimento.

Qualora una o più delle verifiche di cui sopra dia esito negativo, il *customer care* non procede alla richiesta. Inoltre, vengono effettuati alcuni tentativi di chiamata sul numero per verificare l'effettivo stato della linea.

Ad avviso di tale rispondente, il punto di forza del processo, più che nel mero invio dell'avviso via SMS, sta proprio nelle attività di verifica e controllo messe in atto dall'assistenza clienti in *back office* poste a protezione del cliente a fronte di eventuali tentativi di frode.

Tale rispondente ritiene che:

- sia condivisibile l'introduzione di un obbligo di invio di un SMS di avviso in tutti i casi di richiesta di sostituzione della SIM;
- sia opportuno introdurre un obbligo per gli operatori a mettere in atto, nel corso della durata della fase di controllo, ogni opportuna iniziativa per verificare l'attendibilità della richiesta di sostituzione della SIM. Ciò anche al fine di sollecitare gli operatori ad adottare procedure idonee e responsabilizzare gli stessi in caso di contestazione;
- sia condivisibile l'introduzione di un meccanismo di OTP nel caso di richiesta di sostituzione per cambio formato o profilo della SIM (non nei casi di sostituzione di SIM guasta o smarrita/rubata).

In tema di "*SIM business*"

Un rispondente ritiene che il caso di SIM *business* con riserva fredda consegnata al cliente debba essere considerato separatamente e riferisce di mettere a disposizione di tale clientela uno strumento che consente al cliente di richiedere, in piena autonomia, anche la sostituzione di una SIM in caso di smarrimento, mancato funzionamento o necessità di modifica del formato.

In tema di "*Tempo di attesa*"

Tre rispondenti condividono l'obbligo di inviare un messaggio di conferma all'utenza sulla "vecchia" SIM prima di generarne una nuova e la necessità di utilizzare una OTP da comunicare da parte del possessore della vecchia SIM, al fine di contrastare attività fraudolente, nonché la ratio della norma di prevedere o l'esplicita accettazione o, in assenza (SIM smarrita, rubata o guasta), ad esempio, l'introduzione di un adeguato tempo per consentire di informare il cliente dell'imminente cambio SIM e, nel caso di cambio all'insaputa dell'utente, di bloccare il processo. Uno di questi propone che la richiesta dovrà essere confermata dall'utente attraverso inserimento di OTP entro le 72 ore dalla consegna della nuova SIM: decorso tale termine, la richiesta decadrà automaticamente; in base alla medesima ratio, in assenza di conferma l'utenza mobile non dovrà essere attivata.

Alcuni rispondenti ritengono che quanto viene messo in campo non dovrebbe prevedere situazioni che conducono a lunghi periodi di attesa, in quanto questi sono considerati inefficienti e potrebbero prolungare il disservizio al cliente.

Un altro rispondente ritiene che la necessità di rafforzare la sicurezza dei processi non possa avvenire a danno dell'efficienza generale. Pertanto, ritiene che la durata della fase di controllo (corrispondente al principio di attesa proposto), tuttavia, non possa durare più di 30 minuti e non si possa condividere un'ipotesi di 72 ore o comunque di ore.

In tema di "*Blocco della procedura*"

Un rispondente ritiene che il consumatore debba sempre avere la possibilità di bloccare il processo di sostituzione della SIM attraverso una procedura semplice ed uniforme "*anche solo inviando un SMS ad un numero prefissato, concordato tra tutti gli operatori mobili e l'Autorità, con codice "40", ovvero chiamando il customer care e svolgendo la procedura in autonomia o parlando con un operatore, nonché accedendo ad un'area riservata sul sito web dell'operatore*".

Un rispondente ritiene che, qualora l'utente riceva la notifica, ma abbia intenzione di bloccare la procedura, possa inviare un SMS ad un numero prestabilito uguale per tutti gli operatori con codice "40" oppure chiamare il *customer care*, seguendo un iter anch'esso identico per tutti i gestori (es: dal menù guida vocale per procedere al blocco della sostituzione della SIM o per inibire la migrazione verso altro operatore per tutti gli operatori sarà necessario "premere il tasto 3"). In alternativa, l'utente potrà accedere ad un'area riservata sul sito *web* dell'operatore ed evitare la finalizzazione del processo attraverso il portale. Le indicazioni sulle modalità disponibili per interrompere la procedura dovranno essere contenute nel testo dell'informativa trasmessa via SMS o tramite e-mail in fase di attivazione e dovranno, altresì, essere rese note e facilmente reperibili all'interno dei siti degli operatori. Tale rispondente suggerisce, a tale proposito, la creazione di un'area dedicata nei portali dei singoli gestori.

Un rispondente ritiene che la possibilità di bloccare la portabilità da parte del cliente potrebbe dare luogo a fenomeni particolarmente delicati che le attuali procedure di portabilità mobile al momento non consentono.

Un altro rispondente ritiene che nei casi di SIM guasta o smarrita/rubata, deve essere data la possibilità di bloccare la sostituzione mediante la semplice replica all'SMS informativo ricevuto o una chiamata al *call center*. Ritiene sia più efficace ed intuitivo per il cliente, rispetto al numero unico proposto:

- la risposta via SMS al medesimo numero dal quale è stato ricevuto l'SMS di avviso sostituzione;
- una chiamata al *call center*, imponendo eventualmente un obbligo di prevedere sempre una uscita IVR (assistita da operatore) per la richiesta di blocco SIM o blocco sostituzione SIM (come già avviene in altri contesti e mercati, ad esempio

bancari, nei quali è necessario un presidio di sicurezza sull'uso di carte elettroniche).

In tema di "*Segretezza ICC-ID e uso di meccanismi simili alla pre-validazione*"

Un rispondente ritiene che una delle informazioni più complesse da inserire nella richiesta di MNP sia il codice ICC-ID e, al fine di agevolare i clienti nel recupero di tale informazione, propone che gli operatori debbano pubblicare sul sito *web*, nell'area riservata dei clienti, il numero seriale della SIM (ICC-ID), affinché il cliente possa verificarlo e consultarlo anche se sprovvisto del terminale e/o della SIM. Tale rispondente ritiene che nel caso di sottoscrizione a distanza che prevede l'inserimento dei dati direttamente dal cliente, tale soluzione permetta che tale dato sia facilmente copiato senza rischiare di incorrere in errori.

Un altro rispondente ritiene che qualora la pre-validazione venisse estesa a tutti i casi di MNP e non solo ai casi di sostituzione della SIM, renderebbe non più necessaria l'acquisizione di una copia della vecchia SIM oggetto di portabilità. Ciò in considerazione del fatto che, in ragione della presenza di una conferma tramite OTP, a livello di processo non sarebbe più necessario richiedere un controllo sul numero seriale della carta SIM del *donating*.

In tema di "*Contatti alternativi*"

Un rispondente ritiene che la creazione e la manutenzione di contatti alternativi, quale quella proposta, sia il principale ostacolo alla soluzione illustrata. Tale rispondente osserva che l'eventuale fornitura di tali contatti, in sede di richiesta di sostituzione della SIM, non fornirebbe alcuna tutela al cliente intestatario in quanto l'eventuale frodatore fornirebbe contatti alternativi funzionali all'eventuale attività fraudolente.

Un altro rispondente ritiene che sebbene tali misure appaiano astrattamente utili al contrasto dei fenomeni fraudolenti, la evidenziata necessità che «ai numeri mobili "principali" siano associati altri numeri mobili ed e-mail» possa diminuire l'immediatezza ed efficacia della notifica in tutti i casi in cui l'effettivo titolare della SIM non sia nelle condizioni di utilizzare la numerazione mobile alternativa (nei casi, peraltro ragionevolmente limitati, in cui ne abbia la disponibilità) o non abbia accesso alla propria casella di posta elettronica (si pensi all'ipotesi di impossibilità di accedere ad Internet dai propri *device* a seguito proprio del furto o smarrimento della SIM o, addirittura, del *device* stesso).

Un altro rispondente ritiene che sia condivisibile l'ipotesi di invio di un avviso di cambio SIM a tutti i contatti alternativi disponibili per il cliente, inclusa la e-mail ed eventuali numeri telefonici mobili. Ritiene che tale comunicazione sia quella che inneschi la fase di verifica e controllo della richiesta di sostituzione che dovrebbe essere posta in atto da ciascun operatore.

In tema di "*IVR in sostituzione di OTP via SMS o per il blocco*"

Un rispondente ritiene che l'invio di SMS OTP di richiesta conferma allunghi i tempi di sostituzione nei casi di clienti che abbiano realmente smarrito la SIM e non sia sicura in caso di frode, ad esempio, nel caso di persone anziane o che fanno un raro utilizzo degli SMS. Tale rispondente propone, in alternativa all'SMS con OTP, che venga valutata da un Tavolo tecnico l'introduzione di una chiamata automatica al cliente in modo che lo stesso possa bloccare o confermare la sostituzione in modo semplice (es: premere 1 per bloccare, 2 per confermare). I tentativi di chiamata potrebbero essere ogni x minuti (es:15), per 12-24 ore e, in caso di mancata risposta, si potrà procedere alla sostituzione perché verosimilmente la SIM è stata effettivamente smarrita.

Un altro rispondente rappresenta che la procedura adottata dallo stesso per la sostituzione della SIM in caso di furto e smarrimento prevede che vengano effettuati alcuni tentativi di chiamata sul numero per verificare l'effettivo stato della linea. Tutto ciò entro 15 minuti dall'invio di un SMS di avviso. Qualora si riesca a contattare il cliente titolare, e questo non sappia nulla della richiesta, lo si avvisa del tentativo che è stato effettuato e non si dà seguito alla sostituzione.

Valutazioni dell'Autorità relativamente al criterio n. 3

Introduzione di una procedura o basarsi esclusivamente su identificazione dell'utente o su messaggi informativi

L'Autorità ritiene non accoglibile la proposta di basarsi esclusivamente su una corretta identificazione del cliente presso il *dealer* o l'utilizzo solo di messaggi informativi.

Relativamente alla prima proposta, la posizione contraria dell'Autorità si giustifica poiché, nonostante l'obbligo di identificazione è vigente, casi significativi di cambio SIM senza la volontà del cliente si verificano e possono verificarsi anche con la connivenza del *dealer*, per cui le nuove procedure dovranno consentire di arginare anche questi casi.

Relativamente alla seconda proposta che prevede di avvisare il cliente con un SMS di tipo informativo, l'Autorità ritiene che ciò non sia sufficiente e che debba essere in generale accompagnata da altri accorgimenti. Ad esempio, nel caso della MNP e nei casi di cambio SIM senza cambio dell'operatore dove la SIM è in possesso del cliente, occorre un assenso espresso o di altre azioni nel caso di SIM guaste, smarrite o rubate.

L'Autorità, pur essendo conscia che anche con l'uso dell'OTP per dare un assenso espresso da parte del possessore della SIM possano verificarsi casi di cambio SIM indesiderati dovuti all'uso da parte del frodatore di metodi di "*social engineering*", ritiene che sia più sicuro un consenso espresso rispetto ad un'informativa e che i messaggi con cui viene dato l'OTP possano raccomandare di non dare seguito a richieste di conoscere l'OTP da parte di terzi.

L'Autorità ritiene condivisibile la proposta di prevedere che, in caso di SIM smarrita o rubata o guasta, il cliente si possa rivolgere solo all'attuale operatore.

SIM *business*

L'Autorità ritiene condivisibile la proposta di differenziare il caso di SIM *business* con riserva fredda consegnata all'azienda, fermo restando che le procedure adottate siano nel rispetto delle norme vigenti, tra cui quanto sancito dal Codice, all' art. 55, comma 7. Le condizioni minime saranno stabilite da un Tavolo tecnico.

Tempo di attesa

L'Autorità ritiene, altresì, condivisibile la proposta che la richiesta di cambio SIM, nell'ambito della MNP, debba essere confermata dall'utente in risposta all'SMS ricevuto entro un prefissato termine, decorso il quale la richiesta decadrà automaticamente. Ciò al fine di evitare lunghi periodi di attesa. I casi di SIM guasta, rubata o smarrita, sono gestiti esclusivamente dall'attuale operatore e, pertanto, non si verificano nel caso di MNP.

L'Autorità ritiene condivisibile la proposta di individuare procedure che consentano di evitare lunghi periodi di attesa, purché vi sia sufficiente informazione verso il cliente e azioni aggiuntive nel caso in cui il cliente non possa oggettivamente (SIM guaste, rubate o smarrite) fornire l'assenso espresso.

Blocco della procedura

L'Autorità conferma la necessità di introdurre una procedura semplice ed uniforme per bloccare il processo di sostituzione della SIM, rispondendo al messaggio ricevuto ovvero inviando un SMS ad un numero prestabilito uguale per tutti gli operatori con codice "40", chiamando il *customer care*, accedendo ad un'area riservata sul sito *web*. L'Autorità ritiene, altresì, condivisibile la proposta secondo la quale le indicazioni sulle modalità disponibili per interrompere la procedura dovranno essere contenute nel testo dell'informativa trasmessa via SMS e tramite e-mail in fase di attivazione e dovranno, altresì, essere rese note e facilmente reperibili all'interno dei siti degli operatori.

Con riferimento alla preoccupazione espressa da uno dei rispondenti riguardo al fatto che la possibilità di bloccare la portabilità da parte del cliente potrebbe dare luogo a fenomeni che le attuali procedure di portabilità mobile al momento non sono in grado di gestire, si rappresenta che, con la procedura prevista, la portabilità è richiedibile solo in caso di SIM che può rispondere a conferma della volontà di portare il numero da parte del cliente e che la procedura di blocco è effettuata dal *recipient*.

Segretezza ICC-ID e uso di meccanismi simili alla pre-validazione

L'Autorità condivide le osservazioni relativamente al fatto che il codice ICC-ID è un dato complesso da inserire per il cliente e che è facilmente oggetto di copie illecite. L'art. 6 dell'allegato alla delibera n. 147/11/CIR già prevede che, se si usa la validazione parziale, preventivamente all'invio della richiesta di portabilità, il *recipient* nell'ordine inviato al *donating* può indicare che è stata effettuata la validazione parziale e conseguentemente omettere i dati relativi al numero seriale della carta SIM del *donating*.

Considerato che con il presente provvedimento l'Autorità stabilisce l'obbligatorietà della validazione parziale in tutti i casi di cambio SIM, l'espresso consenso del cliente e l'acquisizione e invio del Codice Fiscale, si ritiene che tali misure siano sufficienti ad incrementare la sicurezza e si possa omettere di inserire il numero seriale della SIM.

Contatti alternativi

Con riferimento alle considerazioni di due rispondenti secondo le quali la creazione e la manutenzione di contatti alternativi sia oneroso e il principale ostacolo alla soluzione proposta è che l'uso di contatti alternativi possa diminuire l'immediatezza ed efficacia della notifica, l'Autorità ritiene che la presenza di contatti alternativi possa non essere obbligatoria, anche se auspicabile in generale, nel caso di SIM non utilizzata per servizi M2M/ IoT. Tuttavia, non si ritiene condivisibile che l'eventuale fornitura di tali contatti, in sede di richiesta di sostituzione della SIM, non fornirebbe alcuna tutela al cliente intestatario in quanto l'eventuale frodatore fornirebbe contatti alternativi funzionali all'eventuale attività fraudolente, infatti, i contatti alternativi utilizzabili sono quelli forniti un certo numero di giorni prima della richiesta di cambio SIM, con relativa informativa/controllo da parte dell'utente.

Nel caso di SIM per servizi M2M/IoT, la presenza di contatti alternativi dovrà necessariamente essere prevista, il che comporta che, qualora l'operatore non sia in grado di gestire contatti alternativi, dovrà necessariamente informare il cliente che la SIM non è idonea per essere inserita in apparati M2M o IoT.

L'Autorità ritiene che non sia necessario un sistema di verifica univoco e che soluzioni alternative possono essere utilizzate dagli operatori. Comunque, il cambio SIM, salvo casi eccezionali, SIM guasta, smarrita o rubata senza recapito alternativo (e-mail, numeri alternativi) deve sempre avvenire con conferma esplicita del cliente sul numero principale. Anche l'uso di chiamate appare un metodo utilizzabile efficace. L'Autorità ritiene che non sia sufficiente la sola identificazione del cliente presso il *dealer*.

IVR in sostituzione di OTP via SMS o per il blocco

Si ritiene di accogliere le proposte di utilizzo di chiamate registrate tramite IVR per consentire il blocco ovvero per dare l'autorizzazione in luogo di una risposta all'SMS.

Testo in consultazione relativamente al criterio n. 4

"Nel caso di numeri mobili utilizzati per servizi M2M, verso i quali le comunicazioni testuali sarebbero inefficaci, deve essere concordata ed individuata preventivamente con l'utente la numerazione a cui inviare una OTP per la conferma della propria volontà;"

Sintesi delle osservazioni del mercato sul criterio n. 4

In tema di "Identificazione"

Un rispondente ritiene che l'invio di un SMS di conferma ad una numerazione indicata dal cliente non sia necessaria in quanto le procedure attuali già prevedono l'identificazione del cliente e la consegna della SIM.

In tema di "*Contatti alternativi*"

Un rispondente ritiene ragionevole che qualora fosse previsto un meccanismo che include l'invio di una OTP, l'operatore debba individuare e concordare con il cliente una numerazione da utilizzare per tale meccanismo, anche se al momento non offre servizi M2M.

Un altro rispondente concorda con l'Autorità in merito alla necessità che le comunicazioni testuali per la notifica e la conferma della volontà di sostituzione della SIM, nel caso di numerazioni utilizzate per servizi M2M, debbano essere trasmesse a numeri previamente indicati dall'utente. L'implementazione di tale modalità di comunicazione appare, in effetti, l'unica idonea ad assicurare l'utilità ed efficacia di tali comunicazioni – che diversamente non verrebbero nemmeno visualizzate dall'effettivo utente, ma solo dalla "macchina" in cui la SIM è inserita – ed è, dunque, funzionale ad un rafforzamento della sicurezza dei servizi anche nell'ambito delle attività M2M.

Un altro rispondente ritiene che la misura posta in consultazione sia sproporzionata rispetto allo stesso interesse da tutelare attraverso l'implementazione della stessa, inefficace in molti possibili casi, nonché fonte di oneri rilevanti per gli operatori. Tale rispondente ritiene particolarmente onerosi gli oneri connessi all'acquisizione preventiva e alla gestione dei canali alternativi di contatto, incluse le variazioni di questi ultimi, che a propria volta dovrebbero essere gestite attraverso il medesimo sistema di sicurezza, secondo il modello che l'Autorità ha già ipotizzato nel documento di consultazione.

In tema di "*IVR in sostituzione di OTP via SMS o per il blocco*"

Un rispondente ritiene che l'invio di una OTP non sia necessario e sia complesso da implementare. Tale rispondente propone l'introduzione di una chiamata voce da effettuare al numero del responsabile del cliente azienda delle SIM IoT/M2M.

In tema di "*Autonoma definizione dei processi di notifica e controllo*"

Un rispondente concorda sulla necessità di introdurre, anche nel caso di SIM utilizzate per servizi M2M, un processo di verifica con l'intestatario. Tuttavia, ritiene che, data la natura dei servizi e del rapporto con il titolare delle SIM, ciascun operatore possa autonomamente definire i più opportuni processi di notifica e controllo (inclusi i tempi di attesa).

In tema di "*Stesse procedure del criterio n. 3*"

Un rispondente ritiene che le stesse considerazioni fatte per le numerazioni mobili di tipo personale valgano anche per le numerazioni utilizzate per servizi M2M. Tale rispondente, in relazione al punto 3, ritiene che la misura sia di difficile implementazione e non sembri dare sufficiente garanzia di contrastare efficacemente eventuali frodi a danno dei clienti. Ritiene che la soluzione migliore da mettere in campo per dare comunque maggiore protezione al cliente potenzialmente oggetto di una sostituzione fraudolenta della SIM sia avvisare il cliente con un SMS (di tipo informativo) che sta per avvenire la sostituzione della SIM su cui ha ricevuto l'SMS stesso.

Valutazioni dell'Autorità relativamente al criterio n. 4

Identificazione

Con riferimento a quanto ritenuto da un rispondente relativamente al fatto che sia sufficiente l'identificazione del cliente e la consegna della SIM e che non sia, quindi, necessario l'invio di SMS di conferma, l'Autorità ritiene, come chiarito anche al punto 3, non accoglibile tale proposta in quanto nonostante l'obbligo di identificazione sia vigente, casi significativi di cambio SIM senza la volontà del cliente si sono verificati e possono verificarsi anche con connivenza del *dealer*, per cui le nuove procedure dovranno consentire di arginare anche questi casi.

Contatti alternativi

Relativamente alla considerazione che la proposta sia sproporzionata rispetto allo stesso interesse da tutelare e che la gestione di contatti alternativi sia onerosa, l'Autorità ritiene che, quantomeno nel caso di SIM utilizzate per servizi M2M/IoT, sia necessario utilizzare contatti alternativi, in quanto comunicazioni al numero associato alla SIM sarebbero del tutto inefficaci.

IVR in sostituzione di OTP via SMS o per il blocco

L'Autorità ritiene che la proposta, anche nel caso di SIM per servizi M2M/IoT, di utilizzare canali di comunicazione alternativi all'SMS sia condivisibile, così come già espresso relativamente al criterio n. 3.

Autonoma definizione dei processi di notifica e controllo

Relativamente alla proposta secondo la quale ciascun operatore possa definire in maniera autonoma i processi di notifica al cliente e di controllo, l'Autorità ritiene che le condizioni minime, anche alternative, debbano essere definite, lasciando poi ai singoli operatori di scegliere quali adottare.

Stesse procedure del criterio n. 3

L'Autorità condivide parzialmente la considerazione che per le SIM per servizi M2M/IoT valgano le stesse considerazioni fatte per le numerazioni mobili per comunicazioni interpersonali, in quanto, nel caso di specie, occorre considerare che eventuali comunicazioni dirette a tali numerazioni sarebbero del tutto inefficaci e, pertanto, occorre prevedere comunicazioni a contatti alternativi, preventivamente resi noti dall'intestatario. Qualora non siano gestiti o non siano forniti contatti alternativi occorre avvisare la clientela che la SIM non è idonea per tali servizi.

Pertanto, l'Autorità ritiene, analogamente a quanto previsto per il caso 3, che non sia necessario un sistema di verifica univoco e che soluzioni alternative possono essere utilizzate dagli operatori. Comunque, il cambio SIM deve sempre avvenire con conferma esplicita del cliente. In questo caso si rende indispensabile l'uso di recapiti alternativi, vista l'inutilizzabilità dei numeri primari. Anche l'uso di chiamate appare un metodo efficace utilizzabile. L'Autorità ritiene, per l'effetto, che non sia sufficiente la sola identificazione del cliente presso il *dealer*.

Testo in consultazione relativamente al criterio n. 5

"In generale, in tutti i casi di cui sopra, l'OTP inviata al cliente e il numero seriale della SIM sono gestiti dai sistemi degli operatori e non sono resi accessibili né al dealer né al customer care dell'operatore stesso, in quanto, essendo elementi riservati ed utilizzati per la validazione delle richieste di cambio SIM, la loro diffusione potrebbe essere causa di elusione dei sistemi di sicurezza previsti dalle norme."

Sintesi delle osservazioni del mercato sul criterio n. 5

Due rispondenti ritengono che l'ICC-ID, debba essere necessariamente disponibile al *customer care* e ai *dealer* per varie attività, tra cui quella di *assurance* e associazione MSISDN/ICC-ID, recupero di PIN e PUK etc. Uno dei due rispondenti propone di prevedere per i *dealer* l'oscuramento delle ultime 3 cifre del seriale delle SIM. Per la verifica di tali ultime cifre si potrebbe prevedere una delle seguenti soluzioni:

- inserimento delle stesse da parte del *dealer* e risposta da parte del sistema mediante un Ok o not Ok:

- possibilità di visualizzazione delle stesse solo a fronte di inserimento di *login* e *password* che consentano sempre e in ogni caso di risalire alla persona che ha effettuato l'operazione.

Altri rispondenti, al contrario, non vedono criticità nel non rendere accessibile tale informazione al *customer care* e ai *dealer* dell'operatore al fine di ridurne la diffusione ed eventuali utilizzi impropri. Uno di questi ritiene necessario identificare una soluzione tecnica (criptazione/tokenizzazione del dato) per rendere accessibile al solo personale autorizzato l'informazione relativa al numero seriale della SIM. Ciò al fine di evitare eventuali accessi al dato in chiaro non autorizzati.

Un altro rispondente ritiene non praticabile la completa inibizione dell'accesso al singolo dato da parte degli addetti al *call center* e, comunque, concorda sull'opportunità che siano introdotti meccanismi di sicurezza a protezione di eventuali trattamenti abusivi o illeciti.

Valutazioni dell'Autorità relativamente al criterio n. 5

L'Autorità osserva che per alcuni operatori l'oscuramento del numero seriale della SIM possa costituire un problema. In tali casi, sistemi di criptazione e tracciamento potrebbero mitigare le problematiche anche se non risolvere la problematica. L'Autorità, tuttavia, con il presente provvedimento, ha stabilito l'obbligatorietà della validazione parziale prima dell'avvio della MNP, per cui l'utilizzo dell'ICC-ID non è più un requisito vincolante. Evitando, quindi, l'uso dell'ICC-ID per la validazione nella MNP, la problematicità relativa viene a cadere.

Testo in consultazione relativamente al criterio n. 6

"Il cliente, in generale, è informato dall'operatore a cui si è rivolto, via SMS e via e-mail, delle fasi di fornitura del servizio richiesto, anche in caso di rigetto della richiesta di MNP, riportando le motivazioni descritte nella delibera n. 147/11/CIR".

Sintesi delle osservazioni del mercato sul criterio n. 6

In tema di "Informare il cliente, tramite SMS, non sicuro"

Un rispondente ritiene che entrare nel dettaglio sulle singole motivazioni di eventuali scarti informando il cliente, tramite SMS, non sia sicuro, in quanto tali informazioni porterebbero ad informare l'eventuale frodatore a ripetere la MNP in modo corretto.

In tema di "Il cliente deve chiamare il *customer care*"

Un rispondente ritiene che il cliente debba contattare il *customer care* ed identificarsi per avere le ragioni di un eventuale scarto. Tale contatto con il *customer care* rende più sicura l'identificazione del referente del contratto al quale verrebbero fornite le informazioni

relative allo scarto dell'MNP in maggiore sicurezza, assicurando, inoltre, attraverso il contatto telefonico, anche una maggior chiarezza e dettaglio di informazione rispetto a quelle fornite tramite SMS.

In tema di "Eventi in cui comunicare con il cliente"

Un rispondente rappresenta che già attualmente informa i propri clienti delle varie fasi del processo di MNP attraverso SMS di notifica (sia al proprio numero che al numero portato).

Nel caso di clientela *business*, il cliente riceve SMS di notifica per i seguenti eventi: inoltro della richiesta; esito della richiesta (OK – KO - reitero) il giorno prima della data di passaggio e reitero, andato a buon fine. Nel caso di clientela *consumer*, presa in carico, KO MNP, accettazione richiesta MNP *recipient*, avvenuto passaggio del numero, notifica dell'avvenuto accredito del credito residuo.

Tale rispondente] ritiene non necessario e costoso introdurre altre misure informative.

Anche un altro rispondente rappresenta che attualmente già prevede l'invio di una comunicazione all'utenza con cui la informa dell'avvio e della conclusione positiva o negativa del processo di portabilità del numero mobile. Tale rispondente ritiene che informare i clienti "*delle fasi di fornitura del servizio richiesto, anche in caso di rigetto della richiesta di MNP, riportando le motivazioni descritte nella delibera n. 147/11/CIR*" risulti molto onerosa in termini di implementazione e non rappresenti un beneficio in termini di sicurezza dei processi in questione. Ciò in quanto ritiene che le informative sulle varie fasi di fornitura, così come sulle causali di rigetto, conterrebbero dati di natura tecnica e dettagli non particolarmente utili all'utente per monitorare lo stato della richiesta o valutare le motivazioni del rigetto.

Un altro rispondente ritiene condivisibile l'implementazione di misure che aumentino la trasparenza di detti processi e, pertanto, l'adozione di meccanismi che prevedano una costante e tempestiva informativa via SMS ed e-mail del completamento dei processi di sostituzione della SIM, nonché di portabilità della numerazione.

Un altro rispondente concorda sulla necessità, qualora si verifichino casi di rigetto della richiesta di MNP, che questi siano motivati ex delibera n. 147/11/CIR, e che si proceda a darne tempestiva comunicazione all'utente a mezzo SMS o e-mail.

Un altro rispondente rappresenta che è in fase di implementazione una funzionalità che informa il cliente con un SMS che sta per avvenire la sostituzione della SIM su cui ha ricevuto l'SMS stesso. Per quanto riguarda la MNP, tale rispondente rappresenta che attualmente il cliente riceve un SMS che lo informa della presa in carico della richiesta di portabilità. L'implementazione dell'invio di un ulteriore messaggio che informi il cliente dell'eventuale rigetto della richiesta, con l'indicazione delle motivazioni riportate nella delibera n. 147/11/CIR, richiederebbe importanti sviluppi con tempi e costi da analizzare.

Valutazioni dell'Autorità relativamente al criterio n. 6

Informare il cliente, tramite SMS, non sicuro

L'Autorità non condivide la considerazione che inviare SMS o chiamare il cliente al numero telefonico interessato non sia sicuro, in quanto solo se il frodatore è già in possesso della SIM e abbia accesso alle comunicazioni della stessa potrà leggere o interagire con il *customer care*. In questo caso, è improbabile che il frodatore abbia interesse ad effettuare un cambio SIM.

Il cliente deve chiamare il *customer care*

Relativamente all'ipotesi che il cliente debba chiamare il *customer* care per ottenere informazioni riguardo alla portabilità, l'Autorità ritiene che sia più sicuro una comunicazione che parte dall'operatore (SMS o chiamata da IVR/*customer care*) rispetto al viceversa, considerato che il CLI può essere soggetto a *spoofing* e non garantisce che si tratti del cliente effettivo. L'Autorità ritiene che una comunicazione dal *customer care* possa essere più efficace purché questa contenga le informazioni di rifiuto con almeno lo stesso dettaglio previsto dalla delibera n. 147/11/CIR.

Eventi in cui comunicare con il cliente

Con riferimento a quali dovranno essere gli eventi dei quali il cliente è informato, l'Autorità ritiene che il *recipient* debba informare il cliente nei seguenti casi:

1) immissione nei sistemi del *recipient* della richiesta di portabilità. Il cliente è, altresì, chiamato a confermare la validità della richiesta di portabilità, altrimenti il processo è bloccato.;

2) l'Autorità ritiene non necessarie comunicazioni in relazione alla ricezione da parte del *recipient* della presa in carico da parte del *donating*. Infatti, questo evento non sembra decisivo in quanto non è ancora noto se la richiesta è accettata o rifiutata;

3) ricezione da parte del *recipient* della risposta positiva o negativa alla richiesta di portabilità: si ritiene che questo messaggio sia utile al cliente onde comunicargli le motivazioni del rigetto (almeno con il dettaglio di cui alla delibera n. 147/11/CIR), ovvero, nel caso di validazione positiva, per comunicargli quando avverrà il passaggio.;

4) avvenuto passaggio del numero;

5) notifica dell'avvenuto accredito (in caso di trasferimento del credito residuo) – questo messaggio è necessario per la trasparenza verso il cliente.

I messaggi potrebbero essere sostituiti da una chiamata dal *customer care* o di un IVR, sebbene il messaggio debba essere previsto in caso di insuccesso della chiamata.