

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore MASSIMO MIOLA

Seduta del 10/02/2026

FATTO

Il ricorrente riferisce di aver ricevuto, in data 20 ottobre 2025, un SMS che lo avvisava che era in corso un pagamento di € 4.900,00 e che per bloccarlo avrebbe dovuto contattare un numero, apparentemente riconducibile al numero ufficiale dell'intermediario. Per bloccare tale bonifico, il ricorrente chiamava il numero indicato. In tale sede, il presunto operatore gli intimava di “remotizzare” il proprio *computer*, inserendo i suoi dati di identificazione e l'impronta digitale in APP, in modo da poter compiere le operazioni necessarie per bloccare la frode.

In realtà, con tali operazioni il ricorrente consentiva l'accesso al proprio conto corrente e autorizzava un bonifico istantaneo *online* da Web verso una persona a lui sconosciuta, per un totale di € 14.900,00. Alle ore 16.12 dello stesso giorno il ricorrente riceveva una telefonata da un reale operatore dell'intermediario che, in ragione dell'importo elevato del movimento, aveva provveduto a bloccare sia la carta che la APP, avvisando il ricorrente di essere stato vittima di una truffa sofisticata, presumibilmente basata su *smishing* e *spoofing*. Il ricorrente, pertanto, presentava subito reclamo e denuncia, ma l'intermediario negava ogni responsabilità e rifiutava il rimborso.

Insoddisfatto della prodromica interlocuzione con l'intermediario, il ricorrente si rivolge all'Arbitro per ottenere il rimborso dell'importo che gli è stato fraudolentemente sottratto. Invocando la responsabilità dell'intermediario ai sensi del d.lgs. 11/2010, evidenzia la mancata applicazione di misure di sicurezza rafforzate da parte dell'intermediario. Il ricorrente chiede pertanto al Collegio di condannare l'intermediario alla restituzione dell'importo che gli è stato fraudolentemente sottratto, pari ad euro 14.900,00.

L'intermediario, costituitosi, conferma i fatti che hanno dato origine al ricorso ed evidenzia come la fattispecie sia riconducibile allo schema classico del "*phishing*" nel quale il soggetto, comunicati i propri codici, consente al frodatore di predisporre operazioni, partecipando alla truffa, seppure inconsapevolmente. Nello specifico, il ricorrente ha ricevuto un SMS, non riconducibile all'intermediario, che ha permesso l'accesso al suo Internet Banking e, di conseguenza, la disposizione del bonifico istantaneo in contestazione.

L'intermediario precisa che l'operazione è stata preceduta dalla creazione della provvista, effettuata mediante riscatto di titoli detenuti dal ricorrente, con successivo accredito sullo strumento di pagamento oggetto della controversia ed è avvenuta con autorizzazione prima a mezzo SMS OTP pervenuto sulla utenza telefonica del ricorrente e, poi, con codice ID a mezzo del *device* in uso allo stesso. Sul punto, cita quanto stabilito dal Collegio di Coordinamento nella decisione n. 8671/24.

L'intermediario specifica, poi, che l'operazione in contestazione consiste in un bonifico istantaneo da WEB e autorizzato da APP, la quale risulta correttamente autenticata, registrata e contabilizzata, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi. L'intermediario rappresenta che le operazioni sono state autorizzate tramite SCA e realizzate dallo stesso cliente, seppur manipolato da un terzo, nella convinzione di agire al fine di mettere al sicuro i propri risparmi. In particolare, la SCA risulta esser stata applicata in tutte le fasi, mediante autenticazione a due fattori, appartenenti alle categorie della conoscenza (ovvero la digitazione del codice ** ID) e del possesso (ossia il *device* su cui viene ricevuta la *push* in App). Più precisamente, risulta regolarmente avvenuta la fase di *enrollment*, quella di Log-in nonché quella dispositiva delle operazioni. Ricorda poi che per configurare il sistema autorizzativo, è necessario installare l'App, associare la carta, inserire le credenziali, i dati della carta e l'OTP ricevuto via SMS.

L'intermediario rileva pertanto che le operazioni contestate potevano essere effettuate solo dal titolare o da chi avesse ricevuto i codici, rilasciati anche inconsapevolmente. Ritene dunque che le operazioni non siano in alcun modo riconducibili ad un *vulnus* nel sistema di autorizzazione dell'intermediario, bensì siano frutto esclusivamente dell'incauto comportamento del cliente, che non nega di aver eseguito personalmente le transazioni, seppur vittima di una truffa. Peraltro, esso intermediario ha attivato anche la misura del blocco dello strumento, dopo il compimento delle operazioni.

Ribadisce come l'operazione sia stata eseguita e autorizzata con codice ***ID e a mezzo del dispositivo del ricorrente, a fronte di un SMS non direttamente riconducibile ai canali dell'intermediario. Ciò depone sia per l'estraneità dell'intermediario, che per l'ingenuità e la negligenza del ricorrente, idonee a integrare una sua condotta gravemente colposa.

Nel rammentare le campagne di informativa svolte per la sicurezza delle operazioni di pagamento, effettuate mediante l'utilizzo di più canali informativi, chiede, in virtù degli elementi considerati, di rigettare il ricorso, stante l'accertata regolarità e l'avvenuta corretta autenticazione ed autorizzazione dell'operazione disconosciuta dal ricorrente.

Nelle repliche, il ricorrente, contestando quanto asserito dall'intermediario in sede di controdeduzioni, evidenzia come sia onere dello stesso, ai sensi dell'art. 10 d.lgs. 11/2010, la prova della valida e genuina autorizzazione delle operazioni da parte del cliente e non solo della avvenuta SCA. Nel caso di specie, l'autorizzazione all'operazione è frutto di un errore essenziale e determinante, indotto dagli artifici e raggiri posti in essere dal truffatore, idoneo a viziare il consenso del ricorrente, che non si può ritenere validamente prestato.

Rileva, poi, che dopo aver ricevuto l'SMS (*smishing*), privo di errori grammaticali e di link sospetti, il ricorrente è stato contattato altresì da un numero ufficiale dell'intermediario (*vishing*). In tale contesto, il ricorrente procedeva alla autorizzazione biometrica tramite impronta digitale nella convinzione di mettere in sicurezza i propri risparmi e non di effettuare un pagamento. Alla luce di tale ricostruzione, emerge come la frode non sia riconducibile al classico *phishing*, ma presenti degli elementi tipici anche del *vishing* e dello *spoofing*.

In merito alla ritenuta colpa grave del ricorrente, quest'ultimo eccepisce che la ricostruzione

dell'intermediario non considera tutti gli elementi del caso concreto, ignorando l'avvenuta telefonata proveniente dal numero ufficiale dell'intermediario e la circostanza che il ricorrente ha agito seguendo istruzioni funzionali a bloccare la frode. Evidenza, poi, la sua diligenza nel disconoscere l'operazione il giorno successivo alla frode. Inoltre, il cliente rileva la sussistenza di problematiche nella fase successiva alla segnalazione, in quanto l'operatore dell'intermediario provvedeva al blocco della carta e dalla APP ma non del conto corrente, così consentendo al truffatore di tentare una ulteriore operazione fraudolenta, non andata a buon fine esclusivamente per il superamento dei limiti giornalieri per i bonifici.

In sede di controrepliche l'intermediario contesta quanto *ex adverso* dedotto, evidenziando come non trovi applicazione la disciplina degli artt. 10 e 5 d. lgs. 11/2010 in presenza di operazioni autorizzate dal cliente, come nel caso in oggetto, in cui lo stesso, pur essendo vittima di frode, ha autorizzato l'accesso da remoto al proprio *computer* e le operazioni di pagamento. Né viene in rilievo alcuna disfunzione del procedimento di autorizzazione delle operazioni.

Per il resto, si riporta al contenuto delle controdeduzioni.

Tanto premesso, si rileva quanto segue in

DIRITTO

La controversia attiene alla richiesta di rimborso di somme indebitamente sottratte a seguito di una operazione fraudolenta compiuta *on line*.

Il ricorso non merita di essere accolto.

Preliminarmente, giova rilevare che l'operazione contestata risulta essere stata eseguita il 20/10/2025. Pertanto, essa rientra nell'ambito di applicazione del d.lgs. 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD), come modificato dal D.Lgs. 218/2017, di recepimento della direttiva 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10-*bis* del d. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, il parere dell'EBA del 21 giugno 2019).

Come costantemente rilevato da questo Arbitro, la novellata normativa ha rafforzato il regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utenti, introdotto dal d. lgs. n. 11/2010 ante modifica e ripetutamente evidenziato da numerose decisioni dell'ABF, anche del Collegio di Coordinamento (cfr. decisioni n. 991/2014; n. 5304/2014; n. 3498/2012; n. 21285/2021).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario. In particolare, ai sensi dell'art. 10, comma primo, d. lgs. 11/2010, si stabilisce che, in caso di disconoscimento di un'operazione di pagamento da parte dell'utente, è onere del prestatore di servizi di pagamento provare che la stessa operazione è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; in difetto della prova della corretta autenticazione, viene meno, per il prestatore dei servizi, la possibilità stessa di riferire le operazioni contestate al cliente. L'art. 12, comma 2-*bis* stabilisce, inoltre, che «*salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente*»,

Con specifico riferimento al requisito di autenticazione forte (SCA), L'art. 10-*bis*, comma 1, del d.lgs. n.11/2010 dispone che, in conformità all'articolo 98 della PSD2 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, «*i prestatori di servizi di pagamento applicano*

l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi". L'art. 1, lett. q), del d.lgs. n.11/2010 ("Definizioni") definisce per "autenticazione: la procedura che consente al prestatore di servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore". La definizione di autenticazione forte (SCA) è fornita dalla successiva lettera q-bis), che riprende l'art. 4 del Regolamento 2018/389, specificando che per autenticazione forte del cliente si intende: "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente) che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Ai sensi dell'art. 38 del Regolamento Delegato (UE) 2018/389 della Commissione Europea, tale requisito si applica a tutte le transazioni successive al 14/09/2019. Inoltre, nella *Opinion* del 21 giugno 2019 (EBA-Op-2019-06) l'EBA ha fornito chiarezza sugli elementi utili alla SCA, con un ulteriore livello di dettaglio, attraverso specifici esempi di soluzioni tecniche, per ciascuna categoria di elementi, *compliant* o meno con le disposizioni regolamentari.

Venendo al caso di specie, il ricorrente disconosce una operazione consistente in un bonifico istantaneo effettuato il 20.10.2025 per un importo pari ad € 14.900,00. La provvista per l'effettuazione della citata operazione risulta essere stata costituita mediante il rimborso di buoni dematerializzati sul libretto di deposito intestato al ricorrente, il cui controvalore è stato poi trasferito sulla carta prepagata tramite una operazione di ricarica:

Come emerge anche dalla denuncia all'Autorità di P.S. in data 21.10.2025, il ricorrente dichiara in sede di ricorso di avere ricevuto un SMS che lo avvisava che era in corso un pagamento di € 4.900,00 e che per bloccarlo avrebbe dovuto contattare un numero, apparentemente riconducibile al numero ufficiale dell'intermediario. Per bloccare tale bonifico, il ricorrente chiamava il numero indicato. Nella denuncia, e nelle repliche, il ricorrente viceversa dichiara di avere egli ricevuto una telefonata da un numero apparentemente riconducibile all'intermediario. In tale sede, il presunto operatore gli intimava di inserire i suoi dati di identificazione e l'impronta digitale in APP, in modo da poter compiere le operazioni necessarie per bloccare la frode, e così facendo il ricorrente consentiva l'accesso al proprio conto corrente e autorizzava un bonifico istantaneo.

Secondo gli orientamenti condivisi dei Collegi, l'operazione, quando è eseguita per intero dal pagatore, deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dal D.lgs. n. 11/2010. Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione, come è nel caso delle c.d. operazioni "sotto dettatura". Viceversa, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo deve essere prestato nella forma convenuta tra il pagatore stesso e il prestatore di servizi di pagamento. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.Lgs. 11/2010.

Venendo al caso di specie, il Collegio rileva che dalla ricostruzione fornita dal ricorrente in sede di ricorso e di denuncia emerge che il ricorrente stesso, seppur vittima di un raggiro, abbia fornito un apporto solamente parziale, con l'inserimento dei fattori di autenticazione per autorizzare un'operazione di pagamento già predisposta dal truffatore.

Pertanto, a fronte del disconoscimento dell'operazione di pagamento da parte del ricorrente, come già menzionato, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata

autenticata, correttamente registrata e contabilizzata, ai sensi dell'art. 10, commi 1 e 2, del d.lgs. 11/2010. Nel caso in esame, trova inoltre applicazione l'art. 10-bis, comma 1, del suddetto d.lgs. 11/2010, come modificato, il quale statuisce che i prestatori di servizi di pagamento applichino l'autenticazione forte del cliente qualora l'utente: *a) acceda al suo conto di pagamento online; b) disponga un'operazione di pagamento elettronico; c) effettui qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.* Il Collegio rileva preliminarmente sul punto che, ai sensi del Regolamento Delegato (UE) 2018/389 della Commissione Europea, il requisito di autenticazione forte (SCA) ricorre in presenza di due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza, purché indipendenti tra loro, nonché la presenza di un collegamento dinamico.

Sulla base di quanto dedotto e documentato dall'intermediario, le operazioni sarebbero state autenticate dallo stesso ricorrente tramite il *device* (****3L2G) e l'utenza telefonica precedentemente securizzate. L'originario *enrollment* risulta avvenuto correttamente, nell'aprile 2025, tramite l'inserimento dell'OTP inviato all'utenza del ricorrente. L'accesso Web risulta eseguito tramite inserimento del codice **ID mediante il *device* in precedenza securizzato; tramite quindi un fattore di conoscenza e un fattore di possesso. L'intermediario versa agli atti le evidenze relative agli accessi effettuati in occasione dell'inserimento del bonifico autorizzato tramite app.

L'operazione di pagamento nel caso di specie è stata preceduta da una operazione di rimborso di buoni dematerializzati sul libretto di deposito intestato al ricorrente, il cui controvalore è stato poi trasferito sulla carta prepagata tramite ricarica. Il compimento di tutte queste operazioni preliminari è disconosciuto dal ricorrente che afferma di non averle mai effettuate, quantomeno consapevolmente. L'intermediario evidenzia che le stesse avvenivano tramite autorizzazione prima a mezzo SMS OTP pervenuto sulla utenza telefonica certificata del ricorrente e poi con codice **ID a mezzo del *device* dello stesso. In particolare, allega evidenza in merito alle modalità con le quali tali operazioni sono state effettuate.

Sul punto, il Collegio si richiama al principio di diritto affermato dal Collegio di Coordinamento con la decisione n. 8671 del 23 luglio 2024: *“I pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente”*. Segnatamente, il Collegio di Coordinamento ha evidenziato che, fra le deroghe all'applicazione della SCA contemplate dal Regolamento Delegato (UE) 2018/389, si ritrova l'art. 15 (Bonifici tra conti detenuti dalla stessa persona fisica o giuridica), secondo cui *“I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare gli obblighi di cui all'articolo 2, se il pagatore dispone un bonifico in circostanze in cui il pagatore e il beneficiario sono la stessa persona fisica o giuridica ed entrambi i conti di pagamento sono detenuti dallo stesso prestatore di servizi di pagamento di radicamento del conto”*. Inoltre, nel Considerando n. 10 del Regolamento si esplicita la ratio di tale deroga, disposta in ragione del basso livello di rischio riscontrabile nei “pagamenti da e verso la stessa persona fisica o giuridica con conti presso lo stesso PSP”; mentre il Collegio di Coordinamento ha precisato che, se *“è pagamento l'attività, posta in essere dal pagatore o dal beneficiario, di versare, trasferire o prelevare fondi, tale può considerarsi sia la ricarica sia il giroconto, ancorché eseguiti da e verso lo stesso cliente con conti presso lo stesso PSP”*. Giova rilevare, tuttavia, che, come sancito dal Collegio di Coordinamento con la decisione n. 22745/2019: *«La previsione di cui all'art. 10, comma 2, del d.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente»*.. L'onere della prova della genuinità della transazione, ovvero della frode, dolo o colpa

grave dell'utente ricade quindi sul prestatore del servizio e può ovviamente essere fornita pure per mezzo di presunzioni gravi, precise e concordanti, secondo quanto dispone l'art. 2729 c.c., di un comportamento fraudolento, doloso o gravemente colpevole dell'utente (*ex multis*, cfr. Collegio Napoli, decisione n. 1091/2018). La stessa Corte di Cassazione, a tale specifico riguardo, ritiene che sia ammissibile la prova indiziaria della sussistenza della colpa grave (cfr. Cass. n. 654/2010).

A tale riguardo, il Collegio rileva che, secondo l'orientamento condiviso dei Collegi, molti dei tentativi di truffa posti in essere con modalità telematiche in materia di servizi di pagamento, e riconducibili al c.d. *phishing/vishing*, si svolgono secondo uno schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, SMS o altri strumenti di comunicazione, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza. La diffusione del fenomeno è tale da condurre a ritenere l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa, al punto da considerare l'operazione di pagamento che viene di volta in questione come autorizzata dal ricorrente e, pertanto, a costui opponibile, benché dalla medesima disconosciuta, *"il cliente è vittima di una colpevole credulità"* (Collegio di Coordinamento, decisione n. 3498/2012).

Dalla ricostruzione dei fatti presentata dall'intermediario, emerge che il cliente abbia ricevuto un messaggio da un numero non riconducibile ai canali dell'intermediario. Di seguito, il cliente avrebbe contattato il numero indicato nel messaggio così ricevuto per bloccare il pagamento e in questo modo avrebbe comunicato i propri dati di accesso al conto (cosa che avrebbe permesso ai truffatori di effettuare le operazioni necessarie alla creazione della provvista).

Di diverso e non coincidente è la versione del ricorrente, il quale nel ricorso dichiara di aver ricevuto un messaggio da un numero privato che appariva come proveniente da un terzo intermediario, gestore di strumenti di pagamento (con indicazione di un numero non riconducibile all'intermediario): mentre nella denuncia e nelle repliche asserisce di essere stato successivamente chiamato da un altro numero (06****3322) – effettivamente coincidente con il numero ufficiale dell'intermediario – con cui un presunto operatore lo avvisava dell'operazione "truffaldina" in atto.

A questo punto il ricorrente, facendo affidamento sulla genuinità della telefonata, seguiva le istruzioni impartite dal presunto operatore, ritenendole funzionali al blocco del bonifico di €4.900,00, acconsentendo alla remotizzazione del suo *computer* ed accedendo all'applicazione con i suoi dati personali e l'impronta digitale.

Rileva il Collegio che la diversità di versioni su tale profilo, di non scarso rilievo nella esatta ricostruzione delle modalità dell'operazione fraudolenta, contribuisce a rinvenire i connotati della colpa grave nella condotta del cliente, il quale, contravvenendo a tutte le raccomandazioni volte a custodire con diligenza le proprie credenziali di sicurezza, non ha esitato a comunicarle ad un terzo, rendendo così possibile la realizzazione dell'operazione fraudolenta. Ragione per cui alcun profilo di responsabilità può essere rinvenuto in capo all'intermediario.

Con riferimento ai sistemi di SMS *alert*, il Collegio rileva che sulla base degli orientamenti condivisi dai Collegi è stata confermata la posizione assunta dal Collegio di Coordinamento sul servizio di *SMS-alert*, ritenuto fondamentale presidio di sicurezza a tutela dell'utente, anche in considerazione dell'obbligo di buona fede nell'esecuzione del contratto; pertanto, la mancata attivazione del servizio di *SMS-alert* o altro servizio assimilabile costituisce generalmente un profilo di responsabilità dell'intermediario (da inadeguata organizzazione imputabile esclusivamente al medesimo intermediario), da cui quest'ultimo può andare esente solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Infatti, il Collegio di Coordinamento (decisione n. 24366/19) ha ribadito che: *"Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso"*

concreto".

Venendo al caso di specie, risulta agli atti evidenza dell'*alert* per le operazioni volte a costituire la provvista, al contrario risulta mancare documentazione attestata l'invio di un *alert* per il bonifico istantaneo oggetto di disconoscimento.

Come è noto, secondo l'orientamento condiviso dai Collegi territoriali, trattandosi di un presidio *ex post*, la mancata attivazione, ovvero il mancato funzionamento di tale servizio, sono ritenuti irrilevanti nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'*alert* non potrebbe in concreto limitare il pregiudizio dell'utente.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE