

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 afferma di essere titolare di un conto corrente e di una carta di pagamento allo stesso collegata. Espone che, in data 6 marzo 2025, intorno alle ore 14:00, smarriva il proprio telefono cellulare, su cui era installata l'App necessaria alla gestione del conto e della carta. Rappresenta che, con immediatezza, si recava presso le competenti autorità per sporgere formale denuncia di smarrimento. Non appena rientrato presso la propria abitazione, provvedeva a contattare il servizio clienti dell'intermediario, richiedendo il blocco del conto corrente e della carta di pagamento, operazione effettuata tra le ore 19:32 e le ore 19:34 del 6 marzo 2025.

Il ricorrente riferisce che, nonostante il tempestivo comportamento adottato, soggetti ignoti effettuavano numerose operazioni non autorizzate, tra il 6 e il 7 marzo 2025, per un importo complessivo pari a € 7.498,69. Il ricorrente espone che tali operazioni comprendevano ricariche, trasferimenti di fondi, bonifici istantanei, pagamenti POS, bollettini, prelievi ATM e ricariche telefoniche, tutte eseguite in totale assenza di consenso o volontà. Rappresenta inoltre che diverse operazioni risultano effettuate in data 7 marzo 2025, dunque successivamente al blocco del conto e della carta; circostanza che evidenzia una grave violazione degli obblighi di diligenza e sicurezza gravanti sull'intermediario. Espone in proposito che l'intermediario respingeva la richiesta di rimborso, sostenendo che le operazioni sarebbero state correttamente autenticate e attribuendo la responsabilità al correntista per presunta negligenza nella custodia delle credenziali.

Il ricorrente contesta integralmente tale ricostruzione e rappresenta di non aver tenuto alcuna condotta dolosa o gravemente colposa, precisando che il dispositivo era protetto da codice di blocco, che il PIN

non era custodito unitamente alla carta e che non vi è stata alcuna divulgazione volontaria delle credenziali. Rappresenta che l'intermediario non ha fornito alcuna prova concreta di colpa grave, limitandosi ad affermazioni generiche, in violazione del principio di inversione dell'onere della prova. Il ricorrente deduce che la mancata predisposizione di adeguati sistemi di sicurezza e il rifiuto del rimborso integrale costituiscono violazione degli obblighi contrattuali e normativi. Il ricorrente chiede pertanto la restituzione dell'intero importo fraudolentemente sottratto, pari a € 7.498,69. Chiede altresì la somma di euro 1.000,00, a titolo di risarcimento danni, ed ulteriori euro 1.000,00, per spese legali.

L'intermediario, costituitosi, premette che il ricorrente è titolare di un conto corrente, a cui è associata una carta di debito; l'importo totale delle operazioni disconosciute ammonta ad € 7.498,69. Nel ricostruire la vicenda, osserva che il ricorrente ha provveduto esclusivamente a bloccare la carta di cui era titolare e non il proprio cellulare o la relativa operatività on line. Evidenzia che gli orientamenti arbitrali in merito ai furti non avvenuti con destrezza, come nel caso in questione, riconoscono una grave mancanza di diligenza nella custodia dello strumento di pagamento e del relativo PIN; osserva che, nel caso in esame, i movimenti contestati sono avvenuti lo stesso giorno del furto del cellulare: pertanto, è agevole presupporre che il codice autorizzativo fosse conservato insieme allo stesso.

L'intermediario sottolinea che le operazioni contestate sono state eseguite in conformità dell'art.10 *bis* del D. Lgs. n. 11/2010, ovvero, solo in seguito alla corretta e regolare "autenticazione forte del cliente" mediante "autenticazione a due fattori" appartenenti rispettivamente alle categorie della conoscenza (qualcosa che solo l'utente conosce, ossia la Password personale del Ricorrente) e del possesso (qualcosa che solo l'utente possiede, ovvero nel caso in esame, secondo l'intermediario, la digitazione del *****ID, *rectius* l'app installata su dispositivo certificato), quindi con la presenza di perlomeno due dei tre elementi necessari previsti in materia; peraltro è possibile utilizzare il fattore di conoscenza solo su dispositivi in precedenza abilitati.

Nel caso in esame, l'intermediario evidenzia che sono correttamente avvenute la fase di enrollment della carta del ricorrente al sistema autorizzativo di tipo dinamico, funzionante cioè mediante l'invio di sms di OTP al numero di cellulare dell'istante; la fase di Log-in, nella quale il ricorrente risulta essersi autenticato mediante inserimento del codice ID; inoltre la fase dispositiva delle operazioni oggetto di ricorso è sempre avvenuta tramite SCA, con inserimento del codice ID. L'intermediario illustra poi la modalità di prelievo *cardless*, il cui procedimento consente il prelievo presso i propri ATM senza usare la carta ma solo la APP, inquadrando un codice QR visualizzato sull'ATM.

In merito alla presenza di una procedura caratterizzata da SCA, come previsto dalla normativa, l'intermediario evidenzia che i propri sistemi di autenticazione prevedono una Procedura "primaria", costituita da Push notification in APP e Codice ID; ed una Procedura "secondaria", costituita da One Time Password (OTP) via SMS e Password; nel caso in esame le operazioni dispositive sono state autorizzate tramite procedura primaria. Sostiene che risulta pertanto inconfutabile come sia stata implementata una SCA conforme al dettato normativo, garantendo anche nel caso in esame la sicurezza dei propri servizi, senza che sia emersa alcuna anomalia e/o malfunzionamento delle procedure necessarie per la rispettiva esecuzione.

L'intermediario sostiene che le operazioni, pertanto, potevano essere eseguite soltanto dal titolare dello strumento di pagamento, in possesso del *device*, su cui veniva inviata la notifica in APP per l'inserimento del codice di sicurezza o, in ultima istanza, da un terzo cui potrebbero essere state fornite, anche inconsapevolmente nell'ambito di uno schema fraudolento di *phishing* tradizionale, i codici di sicurezza e la *password* dinamica necessari per l'abilitazione di detta procedura di autenticazione. Atteso che le operazioni sono state autorizzate con il corretto inserimento del codice ID, ritiene che lo stesso fosse conservato insieme al dispositivo trafugato.

L'intermediario evidenzia, inoltre, che il ricorrente lamenta ulteriori prelievi con la APP di altro intermediario, installata sul device oggetto di smarrimento/furto. Ritiene pertanto verosimile che il ricorrente avesse salvate tutte le password sul dispositivo ovvero che lo stesso non fosse protetto da alcun codice di blocco. Segnala infine che il blocco e l'estinzione della carta in questione è avvenuto

alle ore 19:32, del giorno 06/03/2025: pertanto successivamente alle prime operazioni per cui è controversia. Sottolinea che, come dichiarato dalla ricorrente, la carta veniva bloccata, ma non vi è alcuna prova in atti del blocco del device o della posizione on line del cliente. Il device veniva, infatti, modificato solo in data 08/03/2025 alle ore 16:25, ovverosia il giorno successivo alla ultima operazione eseguita con il dispositivo in uso al ricorrente.

L'intermediario chiede quindi il rigetto del ricorso.

Nelle repliche, il ricorrente contesta la ricostruzione fornita dall'intermediario, rilevando che 11 operazioni fraudolente, pari ad un importo complessivo di € 1.967,43 sono state eseguite il giorno 7.03.2025, quindi 12 ore dopo il blocco della carta effettuato dal ricorrente alle ore 19.32 del 6.03.2025. Sulla circostanza di non aver immediatamente "bloccato il device", riferisce che tale condotta non costituisce violazione di alcun obbligo contrattuale o dovere di diligenza e che, pertanto, ha fatto quanto in suo potere per tutelarsi bloccando il conto corrente tempestivamente e sporgendo denuncia-querela alle Autorità. Contesta, pertanto, che molte operazioni consecutive in un solo giorno, di cui otto pagamenti Pago*, tre bollettini e una ricarica telefonica, avrebbero dovuto essere rilevate dall'intermediario come anomale e quindi, predisporre un blocco tempestivo della carta. Specifica, inoltre, che il fatto che le operazioni siano state adeguatamente autorizzate non implica che il titolare abbia effettivamente voluto e autorizzato l'operazione.

Il ricorrente reitera quindi la richiesta di rimborso delle operazioni, di risarcimento dei danni e chiede la condanna agli interessi legali e delle spese legali.

Nelle controrepliche, con riferimento a quanto argomentato in sede di repliche, l'intermediario si riporta a tutto quanto già eccepito, insistendo nel chiedere il rigetto delle domande.

Tanto premesso, si rileva quanto segue in

DIRITTO

La controversia attiene alla richiesta di rimborso di somme indebitamente sottratte a seguito di operazioni fraudolente compiute *on line*.

Il ricorso merita di essere accolto solo in parte.

Preliminarmente, giova rilevare che le operazioni contestate risultano essere state eseguite tra il 06/03/2025 ed il 07/03/2025. Pertanto, esse rientrano 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 n. 20 operazioni di pagamento, indicando un importo totale di € 7.498,69, tutte effettuate tra il 06.03.2025 e il 07.03.2025. Il Collegio rileva che il ricorrente individua specificamente le operazioni contestate, ma quantifica erroneamente l'ammontare complessivo richiesto in restituzione in € 7.498,69, anziché in € 8.122,19 quale risulterebbe dalla somma di tutti gli addebiti.

Come risulta anche dalle denunce sporte presso l'Autorità di P.S. nelle date del 06.03.2025 e del 10.03.2025, si desume che, in data 6 marzo 2025, intorno alle ore 14:00, smarriva il proprio telefono cellulare, su cui era installata l'App necessaria alla gestione del conto e della carta. Con immediatezza, si recava presso le competenti autorità per sporgere formale denuncia di smarrimento e provvedeva a contattare il servizio clienti dell'intermediario, richiedendo il blocco del conto corrente e della carta di pagamento, operazione effettuata tra le ore 19:32 e le ore 19:34 del 6 marzo 2025. Tuttavia che, nonostante il tempestivo comportamento adottato, soggetti ignoti effettuavano numerose operazioni non autorizzate, tra il 6 e il 7 marzo 2025, per un importo complessivo pari a € 7.498,69. Il ricorrente espone che tali operazioni comprendevano ricariche, trasferimenti di fondi, bonifici istantanei, pagamenti POS, bollettini, prelievi ATM e ricariche telefoniche, tutte eseguite in totale assenza di consenso o volontà.

L'intermediario avanza l'ipotesi che le operazioni disconosciute possano essere state eseguite da un terzo che ha usato le credenziali e i codici presenti sul dispositivo smarrito. Evidenzia che il blocco della carta è avvenuto alle ore 19.32 del giorno 06.03.2025. Sostiene che la cliente non avrebbe richiesto, al momento del blocco, la disattivazione del *device* che sarebbe stato modificato, nel profilo utente, solo il successivo 08/03/2025 alle ore 16.25.

Il ricorrente, invece, afferma di aver provveduto a mezzo dell'apposito numero verde non solo al blocco della carta, ma anche al blocco del conto, producendo all'uopo apposite evidenze che risultano, invero, poco esplicative.

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.

Tanto premesso, il Collegio ritiene, come sarà meglio evidenziato nel prosieguo, di procedere all'esame dei log esclusivamente con riferimento alle operazioni eseguite in data anteriore al blocco della carta, pari a complessivi € 6.154,76; omettendo i pagamenti successivi al blocco, che ammontano a complessivi € 1.967,43.

L'intermediario espone che le procedure di autenticazione forte adottate sono due: procedura "primaria": *Push notification* in *app* e Codice *ID; procedura "secondaria": *One Time Password* (OTP) via *sms* e *password*. In particolare, con riferimento alla procedura primaria, utilizzata nel caso di specie, fornisce apposite note esplicative.

Con riferimento alla fase di configurazione ed *enrollment* dello strumento di pagamento nell'applicazione dell'intermediario, risulta versata in atti apposita schermata, che attesta la registrazione della carta di pagamento del ricorrente al sistema autorizzativo di tipo dinamico. L'intermediario chiarisce che non vi è stato alcun cambio utenza dall'*enrollment* della carta fino alla chiusura.

Quanto all'accesso all'App, l'intermediario ha depositato l'estratto informatico dal quale si evince l'accesso in *app* nella data in cui sono state effettuate le operazioni contestate. Da tale documentazione, in particolare, è possibile desumere il nome utente del ricorrente, il *device id* e l'avvenuta autenticazione mediante secondo fattore (step-up) modalità identificativa (codice *ID). Con riferimento alla fase dispositiva, l'intermediario afferma che le operazioni vengono disposte tramite l'inserimento del codice di sicurezza "*ID" al ricevimento della notifica in *app*.

Il Collegio rileva che un sistema così descritto risulta *compliant* con gli *standard* dettati dalla normativa vigente e declinati dall'EBA, prevedendo più fattori riconducibili l'uno alla sfera della conoscenza esclusiva dell'utente (*ID), l'altro a quella del possesso (*app*) (Collegio di Roma, decisione n. 3507/2024).

Per quanto concerne il prelievo *cardless* di € 600,00, l'intermediario afferma che la medesima è stata autorizzata a seguito di challenge scaturita da un QR code e della conseguente autorizzazione in *app* previo accesso con codice ****ID. Dai log relativi al prelievo ATM, emerge l'utilizzo della *app* ma non del codice *ID. Come già deciso da questo stesso Collegio, deve ritenersi provata la SCA di prelievi *cardless* effettuati con il medesimo sistema utilizzato nel caso di specie, valorizzando anche quanto dedotto dalla resistente nelle controdeduzioni. (Collegio di Napoli, decisione n. 298/26).

Con riferimento alle operazioni Pago*, eseguite il 6/3/2025 per complessivi € 276,56, l'intermediario sostiene che sono state autorizzate tramite *app*, la cui SCA è data "dalla login a due fattori", ma non versa peraltro evidenze al riguardo. L'intermediario non versa nemmeno evidenze relative all'applicazione della SCA con riferimento al pagamento POS di € 20,00, del pari eseguito in data 6/3/2025. Ragione per cui queste operazioni non possono considerarsi correttamente autenticate.

In proposito, si evidenzia che secondo il consolidato orientamento dei Collegi, nel caso in cui l'intermediario non abbia assolto all'onere probatorio sull'autenticazione delle operazioni di pagamento contestate dal cliente di cui all'art. 10, comma 1 del D.lgs. 11/2010, il ricorso dovrebbe essere accolto,

posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente; la prova di autenticazione rappresenta, infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente. Con riferimento invece alle operazioni correttamente autenticate, 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).

L'intermediario ritiene al riguardo desumibile che il codice autorizzativo fosse colpevolmente conservato insieme al cellulare dal fatto che le operazioni contestate si sono verificate nel giorno stesso del furto del cellulare e con inserimento del codice *iID, conosciuto dal solo cliente.

Evidenzia inoltre che quest'ultimo lamenta ulteriori prelievi con l'app di altro intermediario, installata sul device oggetto di smarrimento/furto. Ritiene pertanto verosimile che il ricorrente avesse salvate tutte le password sul dispositivo ovvero che lo stesso non fosse protetto da alcun codice di blocco.

A tale riguardo, il Collegio rileva come in capo alla ricorrente gravino taluni obblighi previsti dalla normativa di riferimento in relazione all'utilizzo della Carta per l'esecuzione di operazioni di pagamento, sia anche relativamente alla custodia delle proprie credenziali di accesso e uso della Carta.

In particolare, nell'articolo 7 del menzionato d.lgs. 11/2010 è espressamente previsto, tra le altre cose, che l'utente (i) utilizzi lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro (che ne regola l'emissione e l'uso e che devono essere obiettivi, non discriminatori e proporzionati) e (ii) comunichi senza indugio, secondo le modalità previste nel contratto quadro al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza. Dal citato articolo del D.lgs. n. 11/2010 pertanto emerge inequivocabilmente la condotta attiva che è richiesta al titolare di uno strumento di pagamento. Emerge, dunque, con riferimento ai summenzionati obblighi, gli utenti dei servizi di pagamento sono tenuti a comportarsi in modo diligente, ovvero adottando una condotta rispondente alle esigenze di cautela nonché di attenzione nell'adempimento degli obblighi di custodia e protezione delle credenziali di sicurezza. (nel caso di specie, i codici OTP di volta in volta ricevuti). E' agevole dedurre che nel caso di specie la ricorrente conservasse le proprie credenziali e codici unitamente al proprio cellulare.

Ciò premesso, il Collegio rileva che al fine di valutare la condotta gravemente colposa del cliente, il Collegio di Coordinamento ha sancito che *«si tratta di verificare se la sequenza temporale tra furto e utilizzi fraudolenti posti in stretta successione tra loro sia idonea a fondare la presunzione della sussistenza della colpa grave in capo all'utilizzatore»*; e che *«nella ricostruzione di tale iter, i fatti noti consistono nel furto della carta e nel suo utilizzo immediato e fraudolento; sulla base di tali premesse in fatto deve risalirsi al fatto ignoto consistente nella conservazione del PIN unitamente alla carta e alla relativa facile associazione. È tale comportamento, infatti, che si pone in contrasto con obblighi specifici derivanti dalla legge e dal contratto con il prestatore e che integra ex se la colpa grave dell'utilizzatore»* (così, Collegio di Coordinamento decisione n. 5304/2013; nello stesso senso anche la decisione del medesimo Collegio n. 6168/2013).

Dovendosi riconoscere quindi la sussistenza di una colpa grave in capo al ricorrente, non esente da censure, e tale da configurare un concorso di colpa, è anche la condotta dell'intermediario.

Infatti, l'eccezione mossa dall'intermediario, secondo cui il blocco sarebbe stato richiesto dal ricorrente solo per la carta, e non per lo stesso cellulare, non è in grado di esonerare lo stesso intermediario da responsabilità: questo in quanto il proprio servizio di call center avrebbe dovuto indagare sulle circostanze di fatto, per comprendere come meglio circoscrivere il rischio di frodi. A fronte del furto del *device*, il solo blocco della carta che, in ipotesi, potrebbe essere ancora in possesso del ricorrente, pare evidentemente inappropriato ed ha esposto il cliente al rischio, poi avveratosi, di ulteriori prelievi non autorizzati.

Sul punto, giova richiamare l'art. 8 del D. Lgs. 11/2010, in cui tra gli obblighi a carico del prestatore di servizi di pagamento in relazione agli strumenti di pagamento, è previsto che *questi debba: "impedire qualsiasi utilizzo dello strumento di pagamento successivo alla comunicazione all'articolo 7, comma 1, lettera b)"*.

Pertanto, devono ritenersi restare a carico dell'intermediario le operazioni compiute successivamente al blocco della carta, le quali, a prescindere dalla loro corretta autenticazione, non sarebbero state compiute laddove l'intermediario avesse tempestivamente provveduto a bloccare ogni modalità di utilizzo dello strumento di pagamento. Le operazioni che risultano eseguite dopo il blocco, ovvero compiute antecedentemente, ma per le quali non è stata prodotta traccia dell'autenticazione e che restano a carico dell'intermediario, si quantificano in complessivi € 2.283,49 (€ 2.263,99 per pagamenti + 19,50 per commissioni).

Con riferimento al servizio di *SMS alert* 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"*.

Nel caso di specie, le operazioni oggetto di contestazione sono 20 e sono avvenute tra il 6 e il 7/3/2025. Non risultano versate in atti evidenze di eventuali *sms alert*. D'altra parte, trattandosi di un furto del dispositivo, l'eventuale invio di *alert* non avrebbe potuto limitare il pregiudizio subito dal cliente.

Quanto alla domanda di ridarcimento dei danni, quantificata in euro 1.000,00, essa non merita di essere accolta, in quanto non è supportata da alcuna documentazione atta a provarne la fondatezza.

Con riferimento al pagamento delle spese legali, anche essa quantificata in euro 1.000,00 e non supportata da alcuna documentazione, il Collegio si richiama al Collegio di Coordinamento, che con pronuncia n. 4580/25 del 12/5/2025, ha affermato che il ricorrente può produrre ogni evidenza documentale da cui si possa evincere l'effettività, la funzionalità e la rilevanza della presenza del rappresentante nella gestione del procedimento. In tal senso, diversamente da quanto sostanzialmente sostenuto dal Collegio di Coordinamento nelle richiamate decisioni del 2012 e del 2016, non è richiesto il deposito della parcella, della notula oppure della fattura emessa dal professionista.

Tra i criteri per determinarne la liquidazione si possono considerare la complessità delle questioni giuridiche sostanziali o procedurali che costituiscono oggetto del ricorso, il valore della controversia, il grado di colpevolezza dell'intermediario resistente, il carattere assolutamente necessario dell'attività di assistenza legale, nonché la rilevanza della stessa nella gestione del procedimento.

Pertanto, il Collegio riconosce un rimborso delle spese di difesa legale quantificate equitativamente in euro 300,00.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente alla restituzione dell'importo di € 2.283,00, nei sensi di cui in motivazione. Dispone altresì il ristoro delle spese

di assistenza difensiva nella misura equitativamente stabilita di € 300,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE