

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	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 11/12/2025

FATTO

La ricorrente, titolare di una carta libretto emessa dall'intermediario convenuto, chiede la restituzione dell'importo sottrattogli a seguito di utilizzo fraudolento della carta. In particolare, espone che in data 20.08.2025, rilevava tramite l'App dell'intermediario un ammanco di € 12.100,00 dal proprio Libretto di risparmio, derivante da 25 prelievi ATM effettuati a partire da marzo 2025. Precisa che la carta libretto e il PIN sono conservati in una cassetta di sicurezza, mai spostati, e conosciuti esclusivamente dalla cliente; che dall'attivazione della carta, non ha mai effettuato alcuna operazione sul Libretto, utilizzando una carta prepagata per le spese e gli accrediti ed utilizzava il Libretto esclusivamente per conservazione dei risparmi, non per operazioni di prelievo. Lamenta che, nonostante fosse cliente da 20 anni, l'intermediario non avrebbe segnalato nessuno dei movimenti anomali che raggiungevano il massimale giornaliero e mensile. Pertanto, ipotizza una clonazione della carta.

La ricorrente quindi, rimanendo insoddisfatta dell'interlocuzione avuta in fase di reclamo, presenta ricorso all'Arbitro per ottenere il rimborso della somma sottratta, pari ad 12.100,00, ritenendo di aver adottato tutte le misure di custodia e di non essere responsabile delle operazioni fraudolente.

L'intermediario, costituitosi, si oppone precisando che la ricorrente è titolare della carta libretto n. ***467, collegata al libretto n. ***285 e richiede il rimborso di operazioni di prelievo ATM eseguite dal 25.03.2025 al 12.08.2025. Aggiunge che il 20.08.2025 la ricorrente si avvedeva, utilizzando l'applicazione presente sul suo *smartphone*, di operazioni di prelievo effettuate con il riferito strumento di pagamento. Precisa in proposito che tutti i prelievi sono stati autorizzati con lettura del chip EMV della carta e corretta digitazione del PIN al primo tentativo e nessuna anomalia è stata riscontrata nei sistemi.

Ritiene inoltre improbabile una clonazione, data la presenza di tecnologia EMV e operazioni effettuate in prossimità della residenza della cliente.

L'intermediario, precisando che il blocco della carta è avvenuto solo il 20.08.2025 alle ore 08:32, dopo le operazioni contestate, sottolinea la colpa grave della ricorrente per mancata custodia di carta e PIN, nonché la mancata allegazione di prove concrete sulla dinamica della frode. Ritiene in proposito probabile una sottrazione temporanea della carta e del PIN, il suo utilizzo fraudolento e la successiva ricollocazione nel luogo da dove era stata sottratta, escludendo una clonazione, poiché le operazioni sono avvenute in Italia e non all'estero.

Pertanto, l'intermediario chiede il rigetto integrale del ricorso per infondatezza in fatto e diritto.

La ricorrente nelle repliche sottolinea di essere una insegnante e di utilizzare una carta prepagata emessa dall'intermediario per accredito dello stipendio e spese ordinarie; che il libretto è destinato esclusivamente al risparmio; che - prima dei prelievi contestati, non ha mai effettuato prelievi ATM con unica eccezione per l'attivazione della carta. Ribadisce che la carta è stata sempre conservata in cassetta di sicurezza, con chiave sempre in possesso della cliente, ed i prelievi sono avvenuti in orario lavorativo, incompatibile con un suo utilizzo diretto.

La ricorrente ribadisce la mancata tutela da parte dell'intermediario, che non ha segnalato le operazioni anomale, nonostante l'importo elevato (€ 12.100,00); il numero di prelievi: 25 prelievi in meno di 5 mesi; il profilo di utilizzo del libretto (nessun prelievo precedente). Lamenta anche di non aver ricevuto alcun alert avente ad oggetto l'esecuzione delle operazioni contestate.

Pertanto, la ricorrente ribadisce la richiesta di rimborso integrale dell'importo sottratto.

Nelle controrepliche, l'intermediario si riporta a tutto quanto già eccepito e controdedotto, insistendo nel richiedere il rigetto del ricorso in quanto infondato in fatto ed in diritto.

Tanto premesso, si rileva quanto segue in

DIRITTO

La domanda della parte ricorrente è relativa all'accertamento del suo diritto al rimborso degli importi sottratti a seguito di operazioni fraudolente di prelievo ATM utilizzando la propria carta libretto.

Il ricorso non merita di essere accolto.

Preliminarmente, giova rilevare che le operazioni contestate sono state compiute tra il 25/03/2025 ed il 12/08/2025. 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.

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; da ultimo n. 21285/2021). La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011

Ai fini che interessano la presente decisione, vengono in considerazione le seguenti principali

disposizioni precettive del d. lgs. 11/2010: a) l'art.10, comma primo, 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; b) con riguardo a quest'ultimo profilo, l'art. 8 stabilisce una serie di obblighi gravanti sul prestatore dei servizi, volti a salvaguardare la sicurezza del sistema, primo fra tutti quello di assicurare l'inaccessibilità ai terzi delle credenziali di sicurezza personalizzate, fatti salvi gli obblighi posti in capo all'utente ex art. 7; tale ultima disposizione prevede che *"l'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso [...] e che a tal fine adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo"*; c) in difetto della prova della corretta autenticazione, viene meno, per il prestatore dei servizi, la possibilità stessa di riferire le operazioni contestate al cliente; d) l'art. 10, comma secondo, precisa che, in ogni caso, l'apparente corretta autenticazione non è, di per sé, necessariamente sufficiente a dimostrare la riconducibilità dell'operazione all'utente che la disconosca, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'art. 7, essendo, invece, onere del prestatore dei servizi fornire la prova della frode, del dolo o della colpa grave dell'utente; e) l'art. 12, comma primo, pone a carico del prestatore di servizi di pagamento le perdite derivanti dall'utilizzo dello strumento smarrito, sottratto o utilizzato indebitamente, intervenuto dopo la comunicazione di smarrimento o furto prevista dall'art. 7, comma primo, lett. b); f) l'art. 12, terzo comma, nel prevedere la franchigia di € 50,00, entro la quale l'utente può essere tenuto a sopportare la perdita derivante dalle operazioni compiute prima della comunicazione testé menzionata, fa salva l'ipotesi che l'utente *«abbia agito in modo fraudolento o non abbia adempiuto ad uno o più di cui all'art. 7 con dolo o colpa grave»*, nel qual caso l'intera perdita resta a suo carico; g) 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»*, come definita dall'art. 1, lett. q-bis, necessaria, ai sensi dell'art. 10-bis, quando l'utente accede al suo conto di pagamento on-line, dispone un'operazione di pagamento elettronico ovvero *«effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi»*; h) l'art. 7, comma primo, enuclea gli obblighi gravanti sull'utente abilitato all'utilizzo di uno strumento di pagamento: in particolare, questi è tenuto ad utilizzare detto strumento nel rispetto delle condizioni contrattuali che ne disciplinano l'emissione e l'uso, i cui termini devono essere obiettivi, non discriminatori e proporzionati (comma primo, lett. a); il secondo comma precisa, poi, che, *«ai fini di cui al comma 1, lettera a), l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a proteggere le credenziali di sicurezza personalizzate»*.

Se ne può dedurre, dunque, alla luce di quanto precede, che la disciplina in parola fa discendere un duplice ed alternativo regime di responsabilità per l'utilizzo non autorizzato di strumenti o servizi di pagamento: il primo, in base al quale, rispetto alle operazioni poste in essere anteriormente alla tempestiva comunicazione al prestatore dei servizi, l'utente è tenuto a sopportare la perdita derivante dall'utilizzo non autorizzato dello strumento o del servizio di pagamento nei limiti della franchigia di euro 50,00, rimanendo il resto a carico del prestatore dei servizi; il secondo, che opera nei soli casi in cui l'utente abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'art. 7 d. lgs. 11/2010 con dolo o colpa grave, in base al quale l'utente assume, invece, una responsabilità piena e, conseguentemente, sopporta integralmente la perdita.

Al riguardo, il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce *"un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non*

sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947 del 24.6.2014; in senso conforme: Coll. Coord. decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014.; Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010; Coll. Coord. 21285/2021).

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, la ricorrente disconosce 25 prelievi ATM eseguiti dal 25.03.2025 al 12.08.2025 per un importo totale di € 12.100,00.

Come emerge anche dalla denuncia presentata all'Autorità di P.S., la ricorrente dichiara che la carta libretto è sempre stata in suo possesso e che è custodita in una cassetta di sicurezza nella propria abitazione, a cui ha accesso soltanto tramite codice. L'intermediario evidenzia che gli ATM sono tutti localizzati nello stesso comune di domicilio della ricorrente.

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.

Nel caso in esame, l'intermediario riferisce che il sistema di autenticazione adottato è del tipo MICROCHIP con digitazione del PIN. In ottica SCA, la carta integra l'elemento di possesso ed il PIN l'elemento di conoscenza. A riprova di tale sistema di autenticazione, l'intermediario ha prodotto apposite evidenze, in cui tra l'altro è precisato che la dicitura "PIN" indicata nella colonna "Dati Autenticazione" certifica che al momento della materiale esecuzione delle operazioni i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità.

Tale evidenza mostra che il primo prelievo di € 600,00 è avvenuto con la digitazione immediatamente corretta del codice PIN, ragion per cui i preposti sistemi informativi hanno riscontrato il tentativo di prelievo con "action code" 0, e non con il diverso codice 117, generato automaticamente nel caso in cui venga rilevato un errore nella digitazione del codice; - la dicitura "M" nella colonna "Input Mode" identifica operazioni autorizzate con Microchip.

Il Collegio, peraltro, rileva che sono presenti nel periodo prelievi, non rientranti tra quelli sconosciuti, non andati a buon fine ("esito presa in carico" NOK e "action code" 121 di cui non risulta la decodifica). L'intermediario non riferisce nulla al riguardo, né riporta elenco delle decodifiche.

Giova rilevare 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*, 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 sostiene che ricorre nel caso di specie la colpa grave della ricorrente, per la mancata custodia del PIN nonché la mancata allegazione di prove concrete sulla dinamica della truffa. In particolare, ritiene probabile una sottrazione temporanea della carta e del PIN, il suo utilizzo fraudolento e la successiva ricollocazione nel luogo da dove era stata sottratta. Esclude inoltre la ricorrenza di una clonazione della carta, data la presenza di tecnologia EMV e la circostanza che le operazioni sono state effettuate in prossimità della residenza della ricorrente.

Il Collegio rileva sul punto che, alla luce della posizione espressa dal Collegio di Coordinamento, l'impiego della tecnologia a *microchip* rende l'ipotesi della clonazione, se non di impossibile evenienza, almeno altamente improbabile, facendo ritenere che l'esecuzione delle operazioni sconosciute debba essere ricondotta all'incauta custodia della carta e del PIN da parte dell'utente, salvo che quest'ultimo non fornisca la prova di circostanze tali da far ritenere plausibile l'ipotesi della clonazione (Collegio di Coordinamento, decisione n. 897/14; in termini, Collegio di Coordinamento, decisioni n. 991/14 e 3947/14).

.Di recente, i Collegi territoriali hanno convenuto di confermare l'orientamento consolidatosi a seguito dei menzionati pronunciamenti del Collegio di Coordinamento, precisando che è da escludere la

clonazione della carta di pagamento, con conseguente rigetto del ricorso, qualora l'intermediario abbia dimostrato che le operazioni sono state autenticate tramite *microchip* e con la corretta digitazione del PIN, nonché l'assenza di anomalie. Il Collegio rileva altresì che la ricorrente ha dedotto la intervenuta clonazione della propria carta di debito, ma non ha fornito alcuna prova il propositato. Ed infatti, non risulta sufficiente invocare, da parte della ricorrente, una pretesa clonazione dello strumento di pagamento, dovendo essa *“fornire la prova di circostanze tali da far ritenere quantomeno plausibile l'ipotesi della clonazione, per cui limitarsi a sostenere di non aver mai perso l'uso della carta paventando la clonazione non appare bastevole”*: Collegio di Napoli, decisione n. 9478/2024; decisione n. 252/2025; decisione n. 6686/2025).

A questa stregua, laddove il ricorrente affermi di non aver eseguito personalmente l'operazione e di non avere ceduto a terzi e/o smarrito e/o subito il furto dello strumento di pagamento, l'orientamento consolidato dei Collegi è nel senso che *“è da escludersi la clonazione della carta di pagamento, con conseguente rigetto del ricorso, qualora: l'intermediario abbia dimostrato l'assenza di anomalie; il ricorrente non abbia allegato alcun riferimento descrittivo e circostanziale idoneo a rendere verosimile l'asserita clonazione. Similmente a quanto condiviso a proposito degli utilizzi fraudolenti on line non circostanziati dall'utente, nella fattispecie in esame le mancate allegazioni del cliente rappresentano un elemento da cui il Collegio deve trarre il proprio convincimento circa la colpa grave del ricorrente medesimo”* (così Collegio di Milano, decisione n. 12728/2022). Collegio di Milano, decisione n. 1061/2023).

Inoltre, i Collegi hanno convenuto che tra gli indici della colpa grave può essere incluso l'omesso controllo del conto corrente, cui è associata la carta, per un notevole lasso di tempo, poiché il monitoraggio dell'andamento del conto di appoggio consente al titolare dello strumento di pagamento di avere contezza delle operazioni effettuate tramite la carta e così di intercettare eventuali utilizzi non autorizzati. Si aggiunga che se la realizzazione del furto dello strumento di pagamento in un luogo privato (ad es. abitazione) potrebbe costituire una circostanza idonea al fine di escludere la gravità della colpa del ricorrente, in quanto è plausibile pretendere all'interno di tale luogo una diversa e minore soglia di diligenza, questo non vale nel caso di specie, dato che la ricorrente attesta la particolare cura nel custodire la carta ed il PIN, al punto da conservarli in una cassetta di sicurezza posta nella propria abitazione, i cui codici di accesso sarebbero conosciuti solo da costei.

Le circostanze esposte, unitamente alla mancata allegazione di dettagli su come le operazioni fraudolente denunciate siano in concreto avvenute, induce a ritenere che esse siano ascrivibili esclusivamente alla colpa grave della ricorrente.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE