

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERON

Seduta del 31/03/2026

FATTO

Parte ricorrente riferisce al Collegio l'esecuzione di un'operazione di pagamento fraudolenta eseguita in data 14/07/2025. In particolare lamenta che, malgrado non l'abbia effettuata personalmente, l'intermediario ha dato esito negativo alla sua richiesta di disconoscimento. Parte ricorrente si è resa conto del pagamento in questione chiamando, in quella stessa data, il proprio intermediario poiché allarmata dall'impossibilità di completare un pagamento online per l'acquisto di una "vignetta autostradale digitale" mentre si trovava in auto a K* (Austria), all'ingresso dell'autostrada del B*. In questa circostanza, parte ricorrente tentava di finalizzare con la propria carta di credito l'acquisto online presso la società autostradale A* senza successo, non ricevendo sul proprio cellulare la vignetta richiesta; ritentava quindi l'operazione pensando a un *blackout* di connessione, nuovamente con esito negativo. Contattando l'intermediario, veniva informata che la sua carta era stata clonata e che era avvenuto un pagamento per il valore di circa € 1.280,00, operazione poi dalla stessa disconosciuta. A seguito di tali eventi, parte ricorrente ha immediatamente richiesto il blocco della carta e successivamente sporto denuncia, contestando le motivazioni del diniego al rimborso ricevuto dall'intermediario. Afferma, infatti, di essere stata vittima di una frode informatica riferibile alla tipologia "*man in the middle*" o simili, fatto che a suo avviso dimostrerebbe l'inadeguatezza delle infrastrutture informatiche dell'intermediario.

Parte ricorrente chiede quindi il rimborso di quanto illecitamente sottratto.

L'intermediario, riportato il fatto, controdeduce affermando che parte ricorrente era titolare della carta di pagamento n. 434*, abilitata al servizio di Internet banking e utilizzata per disporre l'operazione oggetto di contestazione. Tale operazione risulta approvata correttamente tramite un sistema di autenticazione forte, nel pieno rispetto dei requisiti SCA e senza che si siano verificati malfunzionamenti o compromissioni dei sistemi. Viene inoltre rilevato che la parte ricorrente non ha mai denunciato lo smarrimento o il furto del proprio cellulare né della carta di pagamento.

In sede di reclamo, a differenza di quanto esposto nel ricorso, parte ricorrente avrebbe indicato il proprio figlio come autore dell'operazione, configurando così un uso indebito delle credenziali che l'intermediario aveva affidato esclusivamente alla titolare; d'altronde, l'operazione disconosciuta è stata disposta dal cellulare abitualmente utilizzato per l'Internet banking, motivo per cui deve considerarsi autorizzata.

Quanto asserito dalla parte ricorrente circa la "vignetta digitale" mai ricevuta non corrisponderebbe al vero: prima della notifica push inviata sul dispositivo in uso alla parte ricorrente alle ore 10:39 del 14/07/2025, con cui sarebbe stato autorizzato il pagamento, era stata regolarmente inviata un'altra notifica alle ore 10:28 dello stesso giorno. Non si sarebbe quindi verificato alcun "blackout di connessione", ma semplicemente, dopo la prima notifica, l'utente non aveva inserito il PIN richiesto, effettuando poi un'ulteriore richiesta di pagamento.

L'intermediario sottolinea infine che la notifica push dell'ultimo tentativo indicava chiaramente un sito differente rispetto a quello di A* e un importo diverso, nemmeno espresso in euro. La parte ricorrente era dunque stata messa in condizione di conoscere i dettagli dell'operazione, ma ha ignorato tali informazioni; nel disconoscere l'addebito, inoltre, non ha fornito prove della responsabilità dell'intermediario né dettagli circostanziati sulla dinamica della frode.

Per queste ragioni l'intermediario chiede il rigetto del ricorso.

Parte ricorrente replica evidenziando come il sito web dove è avvenuto l'acquisto fosse strutturato in modo tale da apparire come il portale ufficiale A*, riproducendone il marchio, la grafica e l'intero percorso di acquisto. Sostiene che, ancorché l'operazione risulti tecnicamente autorizzata, tale autorizzazione non possa essere considerata espressione di una volontà consapevole, poiché resa su un presupposto falso indotto da una truffa informatica. In merito a quanto affermato dall'intermediario circa la ricezione di una notifica completa, la parte ricorrente contesta tale ricostruzione precisando che si sarebbe aspettata una spesa di circa dieci euro e non una serie di numeri e lettere indecifrabili. Specifica, inoltre, di non conoscere il significato della sigla "IDR" riferita alla diversa valuta dell'operazione, avendola scambiata per una stringa alfanumerica indicativa del numero dell'operazione; è stato l'intermediario, contattato dopo il secondo tentativo negativo in data 14/07/2025, a chiarirne il reale significato. Secondo parte ricorrente, gli indizi di anomalia dell'operazione — quali la valuta incongrua, l'importo anomalo, il beneficiario incompatibile e il profilo della parte ricorrente — rendevano l'operazione oggettivamente sospetta, imponendo all'intermediario l'attivazione di presidi rafforzati di prevenzione. L'intermediario avrebbe dovuto infatti verificare agevolmente che la parte ricorrente non possiede esperienza in pagamenti extra-UE o in valute estere, né ha mai compiuto operazioni analoghe, non avendo peraltro speciali competenze informatiche per motivi anagrafici.

Alla luce di quanto esposto, parte ricorrente modifica le domande chiedendo che il Collegio *“riesamini il ricorso; qualifichi l'operazione come autorizzata su presupposto falso, indotto da truffa informatica; escluda la colpa grave in capo alla Ricorrente; accerti un concorso di responsabilità dell'intermediario per insufficiente presidio antifrode; e per l'effetto disponga il rimborso dell'importo contestato o almeno di una sua equa parte”*.

L'intermediario controreplica osservando come la parte ricorrente stessa confermi di aver autorizzato l'operazione contestata, pur sostenendo di non aver espresso tale volontà in maniera consapevole.

Viene precisato che l'operazione disconosciuta è avvenuta su un sito internet terzo, differente da quello dell'intermediario, e che, qualora la notifica ricevuta in data 14/07/2025 avesse presentato indizi di anomalia evidenti e concorrenti, sarebbe stato onere della parte ricorrente verificarne la correttezza prima di procedere con la conferma.

L'intermediario ribadisce di essersi limitato a dare esecuzione a un pagamento regolarmente autorizzato, non potendo sindacare sulle singole operazioni della parte ricorrente in base a quelle pregresse, poiché ciò comporterebbe il rischio di bloccare arbitrariamente pagamenti realmente voluti. Infine, si sottolinea che la notifica push inviata era pienamente descrittiva dei dettagli dell'operazione, contrariamente a quanto sostenuto dalla parte ricorrente.

L'intermediario insiste quindi per il rigetto del ricorso.

DIRITTO

La fattispecie in oggetto concerne la richiesta di rimborso di parte ricorrente di un'operazione di acquisto online, in valuta estera, del complessivo importo di € 1.279,97, eseguita in data 14/07/2025 alle ore 10:40.

In proposito il Collegio constata che l'operazione oggetto di contestazione non rientra nell'ambito di applicazione della disciplina di cui al D.lgs. 27 gennaio 2010, n. 11 (di recepimento della Direttiva sui servizi di pagamento, come modificato dal D.lgs. n. 218/17 in attuazione della direttiva 2015/2366/EU - PSD2), essendo emerso in modo pacifico che la transazione è stata eseguita direttamente dalla parte ricorrente

L'operazione contestata è disciplinata dal D.lgs. 27/01/2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 05.07.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di strong customer authentication (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori:

a) è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / enrollment dell'applicazione / registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni; inoltre la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. Tali elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse;

b) è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di alert.

Peraltro secondo l'orientamento dei Collegi, 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 dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP. 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.

Ciò posto il Collegio constata che sulla base delle evidenze prodotte risulta che l'operazione è stata autenticata tramite: (i) PUSH generata tramite l'APP installata sul dispositivo della ricorrente identificato

dal codice univoco 10* (elemento possesso); (ii) la PUSH è stata validata a seguito della digitazione del PIN "MSG INPUT - authType:PIN" (elemento conoscenza).

Il Collegio, ritenuta provata la SCA da parte dell'intermediario procede a verificare se parte ricorrente abbia agito con colpa grave e se vi sia stato un concorso di colpa da parte dell'intermediario.

In proposito il Collegio osserva che la truffa ha avuto origine da un sito clone di un soggetto terzo, diverso dall'intermediario, al quale parte ricorrente dichiara di essersi collegata in data 14/07/2025 nell'erronea convinzione che fosse il sito dell'operatore autostradale A*, per l'acquisto di una vignetta autostradale. In particolare, parte ricorrente afferma, con valenza confessoria, di aver autorizzato il pagamento online, poiché tratta in inganno dal sito che imitava il merchant A*. La stessa parte ricorrente afferma che l'operazione presentava diversi indizi di anomalia "*evidenti e concorrenti*", tra i quali la valuta indonesiana incompatibile con la finalità dichiarata, l'importo elevato e incoerente, il beneficiario extra UE, affermando che ciò rendeva l'operazione "*oggettivamente sospetta*". Parte ricorrente afferma inoltre che ai fini della valutazione della colpa deve considerarsi la circostanza della sua età avanzata (88 anni). Al riguardo il Collegio osserva che la stessa parte ha dichiarato nel reclamo che l'operazione è stata realizzata dal figlio che si trovava con lei in viaggio e in ogni caso si osserva che secondo l'orientamento ABF l'età avanzata non rileva al fine di escludere la sua colpa grave, considerato che la scelta di utilizzare uno strumento di pagamento alternativo al contante comporta l'accettazione dei rischi connessi. In fine il Collegio constata che il sistema dell'intermediario ha inviato alla parte ricorrente una push autorizzativa del pagamento descrittiva dei dettagli dell'operazione (c.d. notifica "parlante"). Tale notifica va considerata equivalente all'attivazione di un sistema di alert (cfr. Collegio di Palermo, decisione n. 307/2025; Collegio di Torino decisione n. 1344/2023).

Per questi motivi il Collegio, constata la colpa grave di parte ricorrente e l'assenza di responsabilità in capo all'intermediario alla causazione del danno, ritiene il ricorso non meritevole di accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE