

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MELI

Seduta del 31/03/2026

FATTO

Con ricorso pervenuto il 25.11.2025 la ricorrente riferisce di essere titolare di un conto corrente, al quale sono collegati n. 2 strumenti di pagamento, ed esattamente una carta di debito e una carta di credito, emesse rispettivamente da un Intermediario A e da un Intermediario B. In data 07.07.2025, mentre si trovava sul luogo di lavoro, riceveva sulla propria utenza una chiamata proveniente da un numero apparentemente riconducibile all'intermediario A. L'operatore riferiva che le carte erano state clonate e localizzate all'estero per acquisti illeciti. Contestualmente venivano inviati dei messaggi SMS che si incanalavano nella *chat* genuina degli intermediari convenuti. Durante la conversazione telefonica, la ricorrente veniva invitata a disinstallare l'App dell'intermediario dal proprio dispositivo. Contestualmente, i malfattori, ottenuti i codici personali della ricorrente, alzavano i massimali delle carte. Venivano quindi effettuati n. 2 addebiti (rispettivamente, di € 2.800,99 e 2.475,99) a favore di un esercente *online* ubicato all'estero, completati in seguito alla dettatura dei codici OTP da parte della cliente (che li ha comunicati ai truffatori nella convinzione di annullare le transazioni). Terminata la chiamata, la ricorrente prendeva atto di essere stata truffata, notando le notifiche di addebito. Inizialmente la banca aveva proceduto ad un rimborso "salvo buon fine" delle somme frodate, procedendo successivamente allo storno della cifra in data 18.08.2025.

La ricorrente afferma di avere un profilo di utente bancario con operatività standard e conservativa, non registrandosi nei suoi movimenti bancari bonifici o pagamenti di importo rilevante. Contesta che i

sistemi di sicurezza degli intermediari non hanno reagito alle anomalie del caso specifico (incoerenza comportamentale, innalzamento del massimale, accesso da un nuovo dispositivo), registrando passivamente l'inserimento dei codici necessari per il buon esito dei pagamenti.

Chiede, in via principale, di accertare e dichiarare la responsabilità contrattuale ed extracontrattuale dei due intermediari per la mancata adozione di misure idonee a prevenire l'uso fraudolento degli strumenti di pagamento e per la vulnerabilità dei loro canali di comunicazione (SMS/telefono) oggetto di *spoofing*; di accertare l'insussistenza di dolo o colpa grave nella condotta di essa ricorrente, vittima di una frode sofisticata basata su manipolazione tecnica e psicologica che ha viziato il consenso e indotto in errore scusabile; di disporre la condanna dell'Intermediario alla restituzione integrale della somma di € 5.276,98, oltre agli interessi legali maturati dalla data del prelievo (07.07.2025) sino all'effettivo soddisfo; in via subordinata, nella denegata ipotesi di ravvisato concorso di colpa, di limitare la responsabilità della ricorrente alla misura minima di giustizia, tenuto conto della preponderante responsabilità organizzativa dell'Intermediario nella mancata rilevazione delle anomalie transazionali (Art. 1227 c.c.); di condannare l'intermediario al pagamento delle spese di procedura (€ 20,00) e al versamento del contributo dovuto alla Banca d'Italia. Entrambi gli intermediari hanno presentato le controdeduzioni.

L'Intermediario A argomenta che:

- la ricorrente ha eseguito pedissequamente le istruzioni fornite dal sedicente operatore, che le chiedeva di svolgere diverse operazioni asseritamente necessarie per bloccare e disconoscere alcuni tentativi di pagamento anomali;
- l'operazione disconosciuta, tuttavia, appare correttamente disposta ed autorizzata, come provato dai log;
- la dinamica descritta dalla ricorrente non è riconducibile ad un comportamento genuino della banca, come ribadito anche con le diverse campagne informative volte a contrastare le frodi informatiche;
- la ricorrente ha mantenuto un comportamento negligente, dando seguito alle indicazioni impartite e facendo affidamento ad un soggetto del tutto estraneo. Infatti, è ragionevole pensare che la ricorrente, durante la conversazione telefonica, abbia ceduto, oltre ai dati degli strumenti di pagamento, anche i codici OTP necessari a perfezionare il pagamento. In particolare, tali codici sono stati genuinamente inoltrati all'utenza della ricorrente per completare correttamente le operazioni, seppur realizzate fraudolentemente;
- ad ogni modo, la ricorrente sembrerebbe essere stata vittima di una truffa riconducibile al *phishing*, che non parrebbe essere una forma particolarmente sofisticata. Quanto alla telefonata ricevuta, con numero telefonico dissimulato, l'intermediario non può esserne responsabile;
- infine, il sistema di sicurezza adottato dalla banca è pienamente conforma alla normativa in materia e ai livelli di sicurezza nazionale antifrode. Pertanto, l'assenza di cautela da parte della ricorrente, in base che ha consentito la realizzazione della frode, è difficilmente scusabile.

L'Intermediario B, in via preliminare, eccepisce l'inammissibilità del ricorso nei propri confronti, in quanto non preceduto dal reclamo. Nel merito, argomenta che:

- in seguito ad un contatto telefonico, apparentemente riconducibile all'intermediario A, la ricorrente ha ritenuto di seguire le istruzioni fornite dal presunto operatore della banca;
- in seguito alla frode subita, la cliente ha richiesto il blocco della carta, aprendo una pratica di disconoscimento, alla quale seguiva riscontro negativo;
- la cliente sembra essere rimasta vittima di una frode secondo alla tecnica del *vishing*;
- l'esecuzione delle operazioni è imputabile esclusivamente alla cliente, che ha seguito le indicazioni impartite telefonicamente dal soggetto frodatore, disinstallando l'App dal proprio dispositivo e fornendo diversi codici OTP necessari ad autorizzare le operazioni. Gli SMS contenenti i codici OTP che la

ricorrente ammette di aver ricevuto, infatti, rappresentano messaggi genuini, inviati dall'intermediario per poter perfezionare le operazioni dispositive;

- non è chiaro se la stessa ricorrente abbia subito ulteriori condotte fraudolente, tramite cui abbia comunicato le proprie credenziali ai malfattori;
- ad ogni modo, dalla ricostruzione della vicenda, si ritiene che l'adozione di una normale diligenza da parte dell'utente sarebbe stato di per sé bastevole ad evitare la truffa;
- le operazioni di pagamento sono state autorizzate in seguito all'utilizzo di due fattori di autenticazione;
- a ciò si aggiunga che gli SMS contenenti i codici OTP esplicitamente riportavano di non comunicare i suddetti codici a nessuno, specificando altresì l'importo e il beneficiario del pagamento;
- pertanto, la ricorrente ha tenuto una condotta gravemente imprudente, alla quale è esclusivamente riconducibile la responsabilità dell'operazione disconosciuta;
- l'intermediario stesso divulga tramite massicce campagne consigli per evitare che i propri clienti rimangano vittime di truffe *online*.

Con le repliche e le controrepliche, la ricorrente e l'Intermediario A hanno sostanzialmente ribadito le proprie conclusioni.

DIRITTO

La controversia attiene ad una richiesta di rimborso di somme che sono state fraudolentemente sottratte alla ricorrente, attraverso operazioni di pagamento a valere su una carta di debito e una di credito, emesse, rispettivamente, da un Intermediario A e da un Intermediario B.

In via preliminare, il Collegio deve affrontare la questione della legittimazione passiva dei due intermediari.

In sede di ricorso, infatti, parte ricorrente avanza una complessiva richiesta di rimborso di € 5.276,98, nei confronti di entrambi gli intermediari. Specifica però che le operazioni fraudolente sono state effettuate su carte connesse a due circuiti differenti: la carta di debito è emessa dall'Intermediario A, la carta di credito è invece emessa dall'Intermediario B. Con la prima sono stati spesi € 2.800,99, con la seconda € 2.475,99.

Sia l'Intermediario A che l'Intermediario B, preliminarmente, all'interno delle proprie controdeduzioni affermano di articolare le proprie difese con riferimento ciascuno alla propria carta, eccependo, al contrario, il proprio difetto di legittimazione passiva per l'altra operazione contestata ed oggetto di ricorso. In particolare, l'Intermediario A riferisce che l'operazione di € 2.475,99 è stata effettuata da un prodotto che non gestisce, assumendo la qualità di "mero collocatore" del prodotto. Si limita cioè esclusivamente a fornire il servizio di domiciliazione sul conto corrente per l'addebito delle spese effettuate mediante la carta, senza assumere alcun ruolo nella gestione del rapporto contrattuale, né nella prestazione dei servizi di pagamento. Sarà, pertanto, l'Intermediario B dover prendere una posizione difensiva su tale pagamento.

L'Intermediario B, dal canto suo, riferisce di essere coinvolto nel ricorso di cui si tratta esclusivamente con riferimento alla carta di credito di propria emissione, non avendo responsabilità per quanto concerne la carta di debito emessa dall'Intermediario A.

Con le repliche, la ricorrente ha contestato l'eccezione di difetto di legittimazione passiva sollevata dall'Intermediario A con riferimento alle somme prelevate con la carta di credito. Riferisce di percepire ed utilizzare i servizi di pagamento all'interno di un ecosistema unito fornito direttamente dall'intermediario A, che gestisce la visualizzazione dei movimenti, la domiciliazione degli addebiti e l'infrastruttura di sicurezza. A detta della ricorrente stessa, scindere le responsabilità tra i due

intermediari significherebbe frammentare la tutela garantita al consumatore, contrariamente alla *ratio* della direttiva PSD2.

A sostegno di tale tesi richiama la decisione n. 6182/2013 del Collegio di Coordinamento, secondo la quale il rapporto contrattuale tra cliente e banca collocatrice non può essere parcellizzato.

La ricorrente chiede, dunque, che l'intermediario A risponda integralmente del danno da ella subito, in quanto la frode è stata possibile a causa dell'inadeguatezza dei sistemi di monitoraggio degli accessi multicanale.

In sede di controrepliche, l'intermediario A ribadisce di svolgere unicamente attività di collocamento del prodotto e di domiciliazione degli addebiti, non intervenendo in alcuna fase del processo autorizzativo. La domiciliazione, infatti, è un servizio accessorio e meramente esecutivo, che non implica alcuna ingerenza nel rapporto tra cliente ed emittente della carta.

Ritiene il Collegio che l'eccezione sollevata dall'Intermediario A non sia fondata. Con la decisione n. 6182/2013, il Collegio di coordinamento ha osservato che *“Tale eccezione deve essere disattesa sulla base dell’orientamento seguito dai Collegi ABF – anche nell’ottica di effettività della tutela del cliente che è da ritenere posta a fondamento del sistema di risoluzione stragiudiziale delle controversie nel senso della legittimazione passiva dell’intermediario “collocatore” dello strumento di pagamento. In proposito, si è rilevato che “il rapporto tra i tre soggetti coinvolti nella vicenda ben può essere qualificato come unitario in un contesto nel quale la separata gestione delle due funzioni (di credito e di debito) rappresenta solo una modalità esecutiva dell’accordo” (così, ad es., con gli opportuni riferimenti, v. Collegio ABF di Napoli, n. 2758/2011, nonché, anche di recente, n. 4524/2013; v. pure Collegio ABF di Milano, n. 2142/2012). Indubbio rilievo, in proposito, sembra assumere la circostanza dell’essere l’intermediario “collocatore” percepito come immediato e naturale interlocutore del cliente nella gestione del rapporto (cfr., ad es., Collegio ABF di Napoli, n. 2914/2013)”*.

Infondata è anche l'eccezione dell'Intermediario B circa l'assenza del preventivo reclamo. In risposta alla contestazione dell'operazione disconosciuta, l'intermediario B ha indicato le modalità per proporre reclamo, come allegato dalla parte resistente alle proprie controdeduzioni. Orbene, le modalità “formali” secondo le quali l'intermediario ritiene di potere processare un disconoscimento di operazioni possono rilevare ai fini interni, ma, certo, la loro inosservanza non rileva al fine della valutazione dell'adempimento dell'onere previsto dalle Disposizioni sull'ABF per procedere alla presentazione del ricorso. Peraltro, nel caso di specie, è vero che la ricorrente non ha depositato il reclamo che afferma di avere inviato all'Intermediario B il 4.08.2025, ma ella ha depositato un riscontro fornito da detto intermediario il 2.08.2025 e il 4.08.2025.

Venendo al merito, le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. Ai sensi dall'art. 10 del d.lgs. 11/2010, a fronte del disconoscimento di una operazione di pagamento da parte dell'utente, il prestatore di servizi di pagamento (PSP) ha l'onere di provare:

- l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione contestata e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
- il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

Secondo gli orientamenti condivisi dei Collegi (cfr. Collegio di Coordinamento, dec. n. 22745/2019), la prova di autenticazione rappresenta, in aderenza al dato normativo, l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente.

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 dlgs. 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 (v. in particolare il parere dell'EBA del 21 giugno 2019).

Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Parte ricorrente lamenta l'esecuzione fraudolenta di 2 operazioni di pagamento, eseguite il 7.07.2025, tramite le due carte, di debito e di credito, per un totale di € 5.276,98.

Si procede, dunque, a valutare l'esistenza della SCA, sia con riferimento alle operazioni precedenti l'effettuazione dei pagamenti, sia con riferimento a questi.

Con riferimento all'operazione di variazione dei limiti operativi su carta di debito, effettuata alle ore 10:20 del 07.07.2025, l'Intermediario A rappresenta che il sistema di autenticazione forte ha così funzionato:

1. alle ore 10:16 del 07.07.2025 viene effettuato l'accesso da *Web browser*, inserendo le credenziali di conoscenza esclusiva della ricorrente;
2. tale fase di *log-in* viene terminata in seguito alla ricezione di una notifica *push* sul device registrato e l'inserimento del codice PIN;
3. successivamente all'accesso, vengono effettivamente modificati i limiti operativi;
4. il sistema invia un SMS all'utenza telefonica registrata della ricorrente, contenente un codice OTP necessario per autorizzare l'operazione;
5. l'intermediario provvede immediatamente a dare comunicazione alla ricorrente, tramite un SMS di *alert*, dell'avvenuta variazione dei limiti della carta di debito.

Da quanto descritto, i due fattori utilizzati relativi all'accesso sono:

- Conoscenza: inserimento delle credenziali e del codice PIN;
- Possesso: *Push* su *device* registrato.

L'intermediario produce le evidenze, tratte dal sistema informatico interno, che confermano quanto affermato.

Il dispositivo al quale è stata inviata la *push* risulta essere sempre quello del ricorrente e, con riferimento alla variazione dei limiti operativi, vi è evidenza dell'invio del codice OTP tramite SMS. Il numero di cellulare al quale sono stati inviati gli SMS contenenti i codici OTP è lo stesso indicato nel ricorso.

Nel caso di specie, in verità, sembra dunque dimostrato il corretto utilizzo di un solo fattore, a fronte dei due richiesti dalla disciplina in materia di *strong customer authentication*.

Tuttavia, l'operazione è avvenuta nella stessa sessione in cui era stato registrato l'accesso che, come visto, è stato effettuato rispettando i requisiti della SCA. Pertanto, il secondo fattore di autenticazione potrebbe essere considerato il fattore di conoscenza (PIN) inserito in fase di accesso (nel medesimo senso, in un caso analogo, si veda Collegio di Milano, dec. n. 8721/ 2025).

Venendo alla verifica della SCA con riferimento all'operazione di pagamento *e-commerce* di € 2.800,99 effettuata tramite carta di debito emessa dall'Intermediario A, effettuata alle ore 10:23 del 07.07.2025, questo rappresenta che il sistema di autenticazione ha così funzionato: viene inviato, alle ore 10:23, al numero di telefono registrato della ricorrente, un SMS contenente il codice OTP necessario per autorizzare il pagamento disposto *online*.

Dunque, da quanto riferito da parte resistente sembra che sia stato adoperato un unico fattore relativo all'elemento del Possesso, consistente nell'inserimento del codice OTP ricevuto tramite SMS all'utenza

registrata della ricorrente. Vengono prodotte le relative evidenze. Si tratta di un SMS “parlante” contenente esplicitamente la somma del pagamento che si sta autorizzando, oltre che il beneficiario della transazione.

Anche in questo caso viene dimostrato il corretto utilizzo di un solo fattore, a fronte dei due richiesti dalla disciplina in materia di *strong customer authentication*. Tuttavia, diversamente da quanto visto per l'operazione di variazione dei limiti operativi, trattandosi di operazione di acquisto su piattaforma *e-commerce*, questa operazione appare essere indipendente dalla precedente operazione di accesso all'*home banking*, con inserimento dunque solo dei dati della carta e del codice OTP sms.

Sulla base dell'Opinion dell'EBA del 21 giugno 2019, in tali casi i Collegi ABF si sono pronunciati nel senso di ritenere non conforme con la SCA un sistema di autenticazione basato sull'inserimento dei dati posti sullo strumento di pagamento e di un codice dinamico monouso. Infatti, il numero della carta e il codice CCV, essendo riportati in chiaro sul fronte e sul retro della carta, sono potenzialmente conoscibili e accessibili anche da parte di terzi, tanto che l'unico fattore di autenticazione ad assumere rilievo in questi casi è l'invio del codice monouso: il sistema adottato, pertanto, non può considerarsi “multifattoriale”.

Per tale operazione, dunque, difetta la prova della SCA con conseguente obbligo di integrale rimborso dell'operazione di € 2.800,99 a carico dell'intermediario A.

Con riferimento all'operazione di pagamento *e-commerce* di € 2.475,99 effettuata alle ore 10:33 del 07.07.2025, l'Intermediario B rappresenta che il sistema di autenticazione forte ha così funzionato:

1. è stata predisposto tramite canale web il pagamento *online*.
2. il sistema invia all'utenza telefonica registrata della ricorrente un SMS contenente un codice OTP necessario per autorizzare e completare il pagamento.
3. vengono digitati nella pagina di autenticazione dei pagamenti *online* sia il codice segreto K**6 (definito dal cliente in fase di primo accesso alla propria area riservata) sia il codice OTP.
4. il sistema di pagamento verifica la correttezza del codice segreto (codice K**6) e del codice OTP e dà esito positivo al pagamento.

I due fattori utilizzati sono dunque relativi a:

- Possesso: inserimento del codice OTP ricevuto tramite SMS all'utenza registrata della ricorrente;
- Conoscenza: codice segreto (codice K**6).

A riprova di quanto affermato, l'Intermediario B produce le evidenze estratte dal sistema informatico interno.

Il Codice K*6 appare correttamente impostato dalla ricorrente in data 14.04.2021. L'SMS contenente il codice OTP necessario per effettuare il pagamento risulta inviato all'utenza telefonica indicata dalla ricorrente in sede di presentazione del ricorso.

A ciò si aggiunga che il testo dell'SMS era di tipo “parlante”, contenente cioè il l'importo da pagare e l'esercente beneficiario del pagamento.

Pertanto, sulla base delle evidenze prodotte dall'Intermediario B, risulta la fase in oggetto sia stata effettuata nel rispetto della normativa in materia di *strong customer authentication*.

Si può perciò procedere a valutare gli eventuali indici di colpa grave della ricorrente.

Sulla base delle evidenze informatiche fornite dall'intermediario, l'operazione oggetto di analisi appare essere stata effettuata direttamente dal cliente o dal frodatore in seguito alla cooperazione colpevole del primo. D'altro canto, parte ricorrente ammette di aver comunicato i fattori di autenticazione ai soggetti frodatori, nella convinzione di svolgere procedure di blocco di operazioni fraudolenti svolte all'estero. Ella, in particolare, riferisce, in sede di denuncia, che in data 07.07.2025 riceveva alle ore 10:05 una telefonata da un numero apparentemente riconducibile all'Intermediario A, con la quale un

finto operatore di banca la informava che le due carte (di debito e di credito) erano state localizzate in Albania e vi erano sospetti circa loro utilizzi illegittimi. L'interlocutore invitava la ricorrente ad accedere al sito della banca e a disinstallare l'App dal proprio dispositivo, seguendo pedissequamente le operazioni indicate telefonicamente. Intorno alle ore 10:30 la telefonata si concludeva e la ricorrente prendeva atto di aver subito una perdita economica pari ai due pagamenti denunciati.

Si è, dunque di fronte ad una dichiarazione confessoria della ricorrente, che assume il valore di prova legale ex art. 2730 c.c.

La ricorrente allega il registro delle chiamate ricevute, dal quale risulta effettivamente una chiamata pervenuta prima dell'esecuzione delle operazioni di pagamento, da un numero che appare riferibile all'intermediario, anche se corrisponde a quello di una filiale ubicata in tutt'altra città (e regione) ed è diverso rispetto a quello della filiale presso la quale la ricorrente intrattiene i propri rapporti bancari.

In sede di ricorso, la ricorrente riferisce di avere ricevuto anche degli SMS, che deposita, parimenti rivelatisi truffaldini, nella chat della banca. In realtà, si tratta degli SMS genuini con i quali sono stati trasmessi gli OTP per l'effettuazione delle operazioni e i messaggi di *alert* susseguenti il loro compimento.

In sintesi, sulla base di tutte le circostanze rilevate, ritiene il Collegio che la ricorrente – pur vittima di una truffa - abbia agito in modo gravemente imprudente, comunicando per via telefonica al suo interlocutore i codici necessari per ampliare i limiti di spesa delle carte e poi effettuare i pagamenti *online*. Ritiene il Collegio che debba considerarsi dato ormai noto ad un qualunque utilizzatore medio di strumenti elettronici di pagamento che gli intermediari non richiedono mai le credenziali di accesso e che in nessun caso si deve accedere alla eventuale richiesta, da chiunque provenga, della loro comunicazione.

Si aggiunge che, nel caso di specie non sembrano riscontrabili gli indici di anomalia previsti dal DM n. 112/07. Deve essere sottolineato, in proposito, che si è in presenza di due sole operazioni, eseguite con carte diverse gestite da diversi intermediari.

In conclusione, il Collegio accoglie il ricorso, per mancata dimostrazione della SCA, con riferimento all'operazione di pagamento effettuata, con la carta di debito emessa dall'Intermediario A, per € 2.800,99. Tale somma deve essere rimborsata, con i richiesti interessi legali dalla data del reclamo fino all'effettivo saldo.

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario A tenuto a corrispondere l'importo complessivo di € 2.800,99, oltre interessi legali dalla data del reclamo. 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