

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) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SCARANO

Seduta del 14/04/2026

FATTO

La parte ricorrente rappresenta di avere ricevuto, tra le ore 15:04 e le ore 15:15 del 24.09.2025, una serie di notifiche *alert* provenienti dall'intermediario che la avvisavano dell'esecuzione di operazioni fraudolente su un dispositivo diverso dal proprio. In tale frangente venivano effettuate tre operazioni, delle quali soltanto un prelievo di € 1.450,00 eseguito con la carta di debito andava a buon fine. Riferisce inoltre di avere immediatamente provveduto al blocco della carta e di aver presentato denuncia presso le Autorità competenti, oltre aver esperito inutilmente la fase del reclamo. Conclude chiedendo il riconoscimento e il riaccredito dell'importo di € 1.450,00 relativo all'operazione contestata.

Nelle controdeduzioni, l'intermediario riferisce che in data 24.09.2025 veniva attivata l'applicazione bancaria su un nuovo dispositivo, precisando che tale procedimento di installazione richiede

necessariamente l'inserimento di dati a conoscenza esclusiva del cliente. Afferma che le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate mediante il corretto inserimento delle credenziali di accesso e che sussista la colpa grave della ricorrente, la quale avrebbe cooperato con il truffatore in occasione dell'installazione dell'applicazione sul nuovo dispositivo. Eccepisce altresì che la ricorrente non si sarebbe attivata tempestivamente dopo la ricezione degli *alert* via *mail* e che nel modulo di disconoscimento la stessa aveva indicato di avere ricevuto messaggi e chiamate da persone che si fingevano operatori dell'intermediario, senza tuttavia produrre le relative evidenze. Conclude escludendo la sussistenza di malfunzionamenti o intrusioni nei propri sistemi informatici.

La ricorrente, nelle repliche, contesta le argomentazioni dell'intermediario, negando di avere in qualsiasi modo cooperato all'installazione dell'applicazione su un nuovo dispositivo e di avere mai rivelato a terzi le proprie credenziali. Sottolinea altresì che le operazioni contestate sono state autorizzate tramite fattore di riconoscimento facciale, sistema che la stessa dichiara di non utilizzare, e che non ha mai ricevuto né fornito alcun codice OTP. Aggiunge di avere contattato tempestivamente l'intermediario, precisando che il blocco del conto corrente è avvenuto soltanto a seguito di tale chiamata.

L'intermediario, nelle controrepliche, richiama le proprie precedenti difese e insiste per il rigetto del ricorso.

DIRITTO

L'operazione oggetto di contestazione rientra nell'ambito di applicazione del D.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13.01.2018) del D.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno e alla disciplina in materia di *strong customer authentication* (SCA).

Ai sensi dell'art. 10 del D.lgs. 11/2010, è onere dell'intermediario provare che le operazioni contestate siano state correttamente autenticate, registrate e contabilizzate e che non vi siano stati malfunzionamenti dei sistemi; solo successivamente spetta all'intermediario provare dolo o colpa grave in capo all'utilizzatore (Collegio di Coordinamento, decisione n. 22745/2019).

Con riferimento alla SCA, le fonti normative sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del D.lgs. 11/2010, 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.

Nel caso di specie, l'operazione contestata consiste in un singolo pagamento effettuato con carta di debito in data 24.09.2025 alle ore 15:17 per l'importo di € 1.450,00.

Secondo la ricostruzione fornita dall'intermediario, l'esecuzione del pagamento è stata preceduta dalle seguenti operazioni: l'installazione dell'APP sul *device* del truffatore; modifica dei limiti di utilizzo della carta di debito; visualizzazione dei codici PAN e CVV della carta da APP.

L'intermediario documenta che nello stesso giorno del 24.09.2025, alle ore 15:05, il proprio sistema ha registrato l'inserimento del codice cliente, della data di nascita e di tre cifre del PIN da parte di un soggetto che accedeva all'applicazione su un nuovo dispositivo, identificato con i propri riferimenti tecnici. Alle ore 15:06:01 l'intermediario inviava un codice OTP al numero di telefono registrato, il quale veniva correttamente inserito alle ore 15:06:06, con esito di validazione positivo registrato dal sistema. Alle ore 15:06:08 l'intermediario completava l'attivazione dell'applicazione sul nuovo dispositivo, inviando contestualmente una *e-mail* di notifica all'indirizzo associato al conto della ricorrente. I fattori di autenticazione utilizzati per l'*enrollment* del nuovo dispositivo risultano pertanto essere il PIN, quale fattore di conoscenza e il codice OTP inviato via SMS, quale fattore di possesso.

Successivamente, alle ore 15:06:14 la cliente (ovvero il truffatore) si autenticava alla APP tramite il riconoscimento facciale (FaceID), apriva la propria Area Personale e dalle impostazioni cliccava sulla gestione dei dispositivi. Alle ore 15:06:47, cliccava su "Blocca" e l'intermediario processava il blocco dell'applicazione originariamente attiva sul dispositivo della ricorrente fin dal 29.05.2025. E' in atti la schermata di conferma di blocco e il log relativo all'invio, sempre alle ore 15:06:47, della notifica del blocco da parte dell'intermediario all'indirizzo *email* della cliente. Sulla base delle evidenze prodotte risulta pertanto che i fattori di autenticazione utilizzati per l'accesso all'area riservata sono il riconoscimento facciale (fattore di inerenza) e l'APP (fattore di possesso).

Il truffatore disponeva quindi la modifica dei limiti di utilizzo della carta, aumentando tutti i plafond dei limiti di spesa, dei pagamenti POS e dei pagamenti *on-line* da € 1.500,00 a € 5.000,00. Tali modifiche venivano approvate, tramite riconoscimento facciale alle ore 15:12 e successive. Sulla base delle evidenze prodotte risulta pertanto che i fattori di autenticazione utilizzati per tali modifiche sono il riconoscimento facciale (fattore di inerenza) e l'APP (fattore di possesso). L'intermediario documenta altresì l'invio di notifiche *alert* via *e-mail* e notifiche *push* al momento di ciascuna modifica. La ricorrente, nel proprio fascicolo, produce le evidenze delle notifiche ricevute via *e-mail*, risalenti a tale arco temporale.

Analogamente, il truffatore procedeva quindi alla visualizzazione dei codici PAN e CVV della carta di debito, rispettivamente alle ore 15:14:30 e alle ore 15:14:45 mediante riconoscimento facciale (FaceID) quale fattore di inerenza, in combinazione con l'applicazione quale fattore di possesso.

Per completezza, la cliente lamenta che il truffatore abbia aggiunto la propria carta di credito al *digital Wallet*, producendo evidenza della notifica *alert* ricevuta via *email*. L'intermediario al riguardo non produce documentazione, per cui non è possibile determinare l'orario in cui tale autorizzazione sia stata fatta. In ogni caso, la carta che è stata aggiunta al *wallet* non è quella su cui è stata effettuata l'operazione disconosciuta, bensì le due operazioni pari a dollari 1.500,00 e 1.300,00 non andate a buon fine. Altresì non rilevante è la circostanza, evidenziata dalla ricorrente in sede di denuncia, secondo cui il truffatore abbia eseguito un giroconto da un conto corrente intestato alla ricorrente presso il medesimo intermediario al conto corrente oggetto di frode per l'importo di € 3.442,00, non contestato e che in ogni caso è sottratto all'obbligo di SCA (v. Collegio di Coordinamento, decisione n. 8671/2024). Né infine rileva la contestazione della ricorrente di non aver mai attivato il riconoscimento facciale. Al riguardo l'intermediario ha rappresentato che è in fase di *enrollment* che viene data dal sistema la possibilità al cliente di scegliere tra PIN (*Smart Code*) e fattore biometrico.

Riguardo invece all'operazione contestata di € 1.450,00, l'intermediario ricostruisce che la ricorrente (ovvero il truffatore operante sul nuovo dispositivo) accedeva a un portale *online* e predisponava

l'acquisto, inserendo i dati della carta. Alle ore 15:17:00 l'intermediario riceveva i dati della transazione trasmessi dal circuito, tra cui l'identificativo della transazione, il nome dell'esercente, l'importo e il codice cliente. Alle ore 15:17:01 l'intermediario comunicava al circuito che l'operazione sarebbe stata autorizzata tramite notifica *push* (modalità OOB), inviando la notifica *push* allo *smartphone* operativo. Alle ore 15:17:12 l'operazione veniva autorizzata tramite l'applicazione con riconoscimento facciale (FaceID). I fattori di autenticazione utilizzati per l'operazione contestata risultano quindi essere l'applicazione installata sul nuovo dispositivo, quale fattore di possesso, e il riconoscimento facciale, quale fattore di inerenza.

Le evidenze prodotte consentono di verificare i singoli passaggi dell'*enrollment* e dell'autorizzazione dell'operazione fraudolenta che in concreto hanno condotto ai risultati registrati dai sistemi informatici e pertanto la prova della *Strong Customer Authentication* (SCA) deve ritenersi raggiunta.

Quanto alla condotta delle parti e i profili rilevanti per la valutazione della sussistenza o meno della colpa grave dell'utente, la ricorrente afferma di non avere mai autorizzato l'installazione dell'applicazione su un nuovo dispositivo, di non avere rivelato a terzi le proprie credenziali, di non avere mai utilizzato il riconoscimento facciale e di non avere ricevuto né trasmesso alcun codice OTP. Non fornisce tuttavia alcuna indicazione in merito alle modalità con le quali sarebbe avvenuta la frode. Nella denuncia e nel ricorso rappresenta solo di essersi accorta dell'utilizzo fraudolento ricevendo delle notifiche *alert* via *mail* relative all'esecuzione delle operazioni. Quale possibile episodio di anomalia riferisce unicamente di aver effettuato circa un mese prima, il 26.08.2025, un acquisto *online* non andato a buon fine su un sito non più attivo e che a seguito della segnalazione il pagamento era stato rimborsato integralmente dall'intermediario.

Si rileva invece che nel modulo di disconoscimento, la cliente segnala di aver ricevuto messaggi *email* o chiamate fraudolente nonché chiamate o messaggi da persone che si fingevano operatori dell'intermediario. Nessun messaggio civetta o né alcuna registrazione di chiamate sono state prodotte in atti.

Al riguardo, secondo il consolidato orientamento dei Collegi, nelle contestazioni di utilizzi fraudolenti online di strumenti di pagamento in cui l'intermediario abbia offerto la prova dell'autenticazione delle transazioni disconosciute e il sistema di pagamento risulti conforme alla *Strong Customer Authentication*, le mancate allegazioni del cliente sulle circostanze di fatto della frode che afferma di avere patito, rappresentano un elemento dal quale il Collegio può trarre il proprio convincimento circa la colpa grave del cliente medesimo, unitamente ad altre circostanze. In particolare, i Collegi sono concordi nel ritenere che la mancata allegazione del messaggio civetta – ovvero, per il *vishing*, del registro delle chiamate - debba determinare il rigetto del ricorso, in quanto non consente di verificare se il mittente o il chiamante risultino riconducibili all'intermediario e se sia quindi configurabile un legittimo affidamento dell'utente circa la genuinità del contatto ricevuto.

Con riferimento alla posizione dell'intermediario e i doveri di protezione dell'utente sullo stesso gravanti, tra cui l'onere di fornire il servizio di SMS *alert* o assimilabili (v. Collegio di Coordinamento, decisione n. 8672/2024), nel caso in esame è stato documentato l'invio di notifiche *alert* sia via *e-mail* che tramite notifiche *push* al momento dell'esecuzione dell'operazione disconosciuta.

Riguardo a queste ultime, è stato stabilito che qualora la truffa sia stata resa possibile dall'*enrollment* del dispositivo del truffatore, le notifiche *push* non possono essere considerate equivalenti agli SMS *alert*, poiché dopo l'avvenuto *enrollment* le *push* vengono inviate al dispositivo del truffatore e non al titolare del conto (Collegio di Milano, decisione n. 13320/2022).

Nel caso in esame, tuttavia, la ricorrente conferma di avere ricevuto notifiche *alert* via *e-mail*. Inoltre, oggetto di contestazione è un'unica operazione fraudolenta, avvenuta alle ore 15:17. Secondo il consolidato orientamento dei Collegi, deve essere adottata un'interpretazione sostanzialistica del

servizio di SMS-*alert*, considerata la sua natura di presidio di sicurezza ex post, con la conseguenza che la mancata attivazione ovvero il mancato funzionamento di tale servizio (o di servizio assimilabile) deve ritenersi irrilevante 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 (v. ex multis, Collegio di Milano, decisione n. 1110/2023),

In conclusione, alla luce di tutto quanto esposto, ritenuto che la condotta della ricorrente risulti caratterizzata da colpa grave, atteso che l'esecuzione dell'*enrollment* del nuovo dispositivo ha richiesto dati personali a conoscenza esclusiva della cliente — tra cui il codice cliente, la data di nascita, il PIN e il codice OTP inviato al numero di telefono registrato — e che la ricorrente non ha fornito alcuna spiegazione circa le modalità con le quali il truffatore sarebbe entrato in possesso di tali credenziali, né ha prodotto evidenza del messaggio civetta o del registro delle chiamate ricevute, indispensabili per valutare la sussistenza di un legittimo affidamento; ritenuto altresì che non ricorrono a carico dell'intermediario inadempimenti causalmente rilevanti rispetto al danno lamentato, il ricorso deve essere rigettato.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE