

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SCARANO

Seduta del 20/01/2026

FATTO

Con il ricorso in esame la parte ricorrente ha dedotto di aver subito un utilizzo fraudolento della propria carta di debito, lamentando la sottrazione dell'importo complessivo di € 435,27 a seguito di una operazione di pagamento online che assume di non aver autorizzato. Ha rappresentato di essersi accorta dell'addebito e di aver tempestivamente contattato l'intermediario, il quale le avrebbe suggerito di procedere al blocco della carta e di presentare il modulo di disconoscimento corredato da denuncia all'autorità competente. La ricorrente ha ricondotto l'accaduto a una asserita clonazione dello strumento di pagamento, precisando che la carta era sempre rimasta in suo possesso.

L'intermediario, costituitosi nel procedimento, ha ricostruito le modalità dell'operazione contestata, evidenziando che la stessa consiste in un unico pagamento eseguito in data 04.07.2025 alle ore 21:35,

su commercio elettronico sicuro per l'importo di € 426,73, cui si aggiungevano commissioni di “*conversion fee*” e di “*optional fee*” per € 8,52, con un addebito totale di € 435,27. L'operazione originava da un importo espresso in moneta dirham degli Emirati Arabi Uniti, convertito in euro al tasso applicabile al momento della transazione.

Secondo quanto dedotto dall'intermediario, l'operazione sarebbe stata correttamente autorizzata tramite il servizio di internet banking, mediante un sistema conforme alla *strong customer authentication*, con utilizzo delle credenziali della ricorrente e del *device* a lei abitualmente riconducibile. In particolare, l'intermediario ha affermato che l'autorizzazione sarebbe avvenuta a seguito dell'invio di una notifica *push* sul dispositivo, contenente la descrizione dell'operazione, e della successiva validazione mediante credenziale dinamica OTP e fattore biometrico. Le tracciate prodotte indicherebbero l'assenza di anomalie e la corretta esecuzione dell'operazione.

L'intermediario ha inoltre rilevato che, in sede di disconoscimento, la ricorrente aveva dichiarato di essere stata contattata nei giorni precedenti da soggetti terzi mediante sms, circostanza che, unitamente alla mancata denuncia di smarrimento o furto del dispositivo, renderebbe verosimile l'ipotesi di una cessione delle credenziali. Da ciò, parte resistente ha fatto discendere la sussistenza di una condotta gravemente colposa della ricorrente, idonea a escludere il diritto al rimborso.

In sede di repliche la ricorrente si è limitata a ribadire le proprie doglianze, depositando nuovamente il modulo di disconoscimento e la denuncia già prodotti con il ricorso introduttivo.

L'intermediario, nelle controrepliche, ha richiamato integralmente le difese svolte e ha insistito per il rigetto del ricorso.

DIRITTO

L'operazione contestata 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 è unica, di importo complessivo di € 435,27, eseguita in data 04.07.2025 alle ore 21:35.

Risulta che la ricorrente ha presentato denuncia il giorno successivo all'operazione, riferendo di essersi accorta dell'addebito il 04.07.2025 verso le 21:30, accedendo al servizio di internet banking a seguito di una ricarica non andata a buon fine e di aver ricevuto successivamente al blocco della carta, lo stesso 04.07.2025 alle 21:42 una notifica dall'App della Banca che la informava di un tentativo di pagamento di 3.673,00 AED (cioè € 850,70). Non fornisce tuttavia elementi circostanziati sulla dinamica della asserita truffa.

L'intermediario ha prodotto log informatici e tracciate dai quali risulta che l'operazione di pagamento on line è stata autorizzata tramite la procedura che prevede l'invio di una notifica *push* sul dispositivo identificato con codice univoco abitualmente utilizzato dalla ricorrente e la validazione del codice OTP previo riconoscimento biometrico ("authType": "TOUCH"). L'operazione si è pertanto perfezionata rispettando i requisiti di inerenza, costituito dal codice OTP generato a seguito di riconoscimento biometrico rintracciabile nella evidenza "*deviceFingerprint*" e di possesso del *device* della cliente identificato dal codice univoco.

Tali elementi, valutati complessivamente, consentono di ritenere raggiunta la prova della corretta autenticazione dell'operazione secondo i requisiti della *strong customer authentication*, non emergendo indizi di anomalia tecnica né profili di malfunzionamento dei sistemi dell'intermediario. Come ricordato, in conformità all'orientamento espresso dal Collegio di coordinamento con decisione n. 22745 del 10 ottobre 2019, la prova dell'autenticazione costituisce presupposto logico necessario per procedere alla valutazione della condotta dell'utilizzatore ai fini dell'accertamento della colpa grave. Sotto tale profilo, rileva che la ricorrente non ha fornito una sufficiente ricostruzione specifica delle modalità con cui i terzi truffatori avrebbero acquisito le credenziali necessarie all'esecuzione

dell'operazione, limitandosi ad allegare una generica ipotesi di clonazione della carta. Al contempo, in sede di compilazione del modulo di disconoscimento, la stessa ha assentito al punto in cui si domanda se il 04.07.2025 o nei giorni precedenti abbia ricevuto sms, email o telefonate da presunti operatori bancari, precisando che si trattava di SMS. Dette circostanze, unitamente all'assenza di denunce di furto o smarrimento del dispositivo e alla regolare autenticazione dell'operazione, consentono di ritenere plausibile un comportamento gravemente imprudente della ricorrente nella gestione delle credenziali di sicurezza.

Secondo l'orientamento consolidato dei Collegi, una volta accertata la sussistenza della *strong customer authentication*, le mancate allegazioni dell'utente sulle concrete modalità della frode e le dichiarazioni rese dallo stesso possono essere valorizzate, unitamente agli altri elementi di causa, per fondare il convincimento circa la colpa grave. Parimenti, la mera evocazione della clonazione dello strumento di pagamento, in assenza di riscontri oggettivi e a fronte di operazioni regolarmente autenticate, non è idonea a superare le risultanze istruttorie.

Non assumono rilievo decisivo, nel caso di specie, né la mancata evidenza di un servizio di *alert* attivo, trattandosi di una singola operazione, né ulteriori profili accessori, quali il plafond di spesa o la franchigia, non specificamente contestati.

Alla luce di quanto sopra, deve ritenersi che l'intermediario abbia assolto l'onere probatorio su di esso gravante in ordine alla corretta autenticazione dell'operazione e che dagli elementi complessivamente acquisiti emerga una condotta gravemente colposa della ricorrente, idonea a escludere il diritto al rimborso dell'importo contestato; ne consegue il rigetto del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE