

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore MASSIMO CARATELLI

Seduta del 14/01/2026

FATTO

1. La controversia verte sulla contestazione di alcuni addebiti operati a valere su di una carta di pagamento, rilasciata dalla resistente e di cui la proponente è titolare.
2. In particolare, in base alla dinamica riferita da parte attrice, l'istante – in data 14 febbraio 2025, verso le ore 19.10, mentre passeggiava – subiva il furto del cellulare. Subito dopo la sottrazione, tramite il suddetto device, tra le 19.37 e le 20.09, venivano effettuati sette pagamenti contactless indebiti, utilizzando la carta bancomat digitalizzata sul wallet del telefono. Precisa la proponente che il device risultava protetto da Face ID e da PIN, distinti sia per lo sblocco dell'apparecchio che per l'utilizzo del bancomat. Tali codici segreti non erano memorizzati sul telefono. Tanto premesso, la ricorrente chiede il rimborso del controvalore delle operazioni non autorizzate, per un totale di euro 1.142,00.
3. Con le controdeduzioni la resistente rileva che qualora la cliente avesse provveduto all'immediato blocco della carta registrata sul wallet, avrebbe verosimilmente evitato le

operazioni effettuate nei circa 27 minuti successivi al furto, trattandosi di un lasso temporale ragionevolmente sufficiente per contattare il numero verde e procedere al blocco dello strumento di pagamento. La carta, invece, veniva bloccata soltanto alle ore 21.27, circostanza che – ad avviso dell'intermediario – evidenzierebbe un comportamento negligente della ricorrente. Al contempo, evidenzia l'istituto di credito che ogni operazione di pagamento effettuata tramite wallet installato su smartphone richiede l'utilizzo di almeno uno dei seguenti fattori di autenticazione: Face ID, Touch ID o codice di sblocco del dispositivo. Tali dati rientrano tra quelli biometrici, nella disponibilità esclusiva del titolare degli strumenti di pagamento. Inoltre, l'inserimento o la modifica dei dati biometrici sul dispositivo presuppone in ogni caso la conoscenza del codice di sblocco, con la conseguenza che, in assenza di tale codice, non c'è possibilità alcuna di variare le impostazioni biometriche. In merito, la stessa controparte, nel ricorso, dichiara che lo smartphone era protetto sia da riconoscimento facciale (Face ID) sia da diversi PIN di sicurezza. Tale circostanza rende assolutamente impossibile l'utilizzo del dispositivo da parte di terzi non autorizzati. Considerato, infine, che la sottrazione del dispositivo parrebbe essere avvenuta in un luogo affollato, l'intermediario ravvisa profili di colpa grave in capo alla ricorrente, sia per la negligente custodia dello smartphone sia per l'inadeguata protezione dei codici di sblocco del telefono.

DIRITTO

1. Ai fini della decisione, vanno anzitutto considerate quali siano le eventuali responsabilità ascrivibili alle parti, alla luce dei criteri indicati dal d.lgs. 27 gennaio 2010, n. 11, che regola la materia dei servizi di pagamento nel mercato interno, così come modificato dal d.lgs. 15 dicembre 2017, n. 218, che ha recepito la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. "PSD 2").
2. Ciò posto, facendo riferimento in via analogica alle decisioni dei Collegi in tema di furto dello strumento di pagamento, occorre anzitutto rilevare che l'aver lasciato incustodito uno strumento di pagamento – o i relativi codici dispositivi – *"alla mercé di terzi"*, senza adottare particolari cautele per prevenire la sottrazione, configura, ad avviso del Collegio, una colpa grave per violazione del disposto di cui art. 7 del d.lgs. n. 11/2010 (cfr. Collegio di Roma, decisione n. 2114/2024). A tale riguardo, si osserva che, nel caso di specie, la parte ricorrente non descrive né allega alcuna circostanza che possa spiegare come possa essere intervenuto lo sblocco del dispositivo sottratto, contenente la carta tokenizzata, nonché l'autorizzazione delle relative transazioni, senza la sua collaborazione o, comunque, senza una sua negligenza;

tali circostanze inducono questo Collegio a ritenere provata, pur in via presuntiva, una violazione da parte della ricorrente dei suoi obblighi di diligente custodia delle credenziali riservate, secondo una condotta che può ritenersi connotata da colpa grave (cfr. Collegio di Roma, decisione n. 12373/2024).

3. Al contempo, si segnala che, tra gli obblighi a carico dell'utente dei servizi di pagamento ai sensi dell'art. 7 del d.lgs. n. 11/2010, rientra anche quello di comunicare "*senza indugio*" lo smarrimento, il furto, l'appropriazione indebita o l'utilizzo non autorizzato dello strumento di pagamento. Sul punto, questo Collegio ritiene che il ritardo nel blocco dello strumento costituisca indice di una condotta negligente dell'utilizzatore, soprattutto nei casi in cui – come nella fattispecie in esame – un intervento tempestivo avrebbe verosimilmente impedito il compimento di ulteriori operazioni (cfr. Collegio di Roma, decisione n. 1033/2023).
4. Sotto diverso profilo, si rileva che la banca ha offerto riscontro del procedimento seguito per autorizzare le operazioni disconosciute, producendo i relativi log, con buon fine della digitazione dei codici. Ne consegue il Collegio che il sistema di autenticazione adottato in fase dispositiva appare in grado di garantire un elevato livello di sicurezza (cfr. Collegio di Coordinamento, decisione n. 9559/2024).
5. Peraltro, non si rilevano nella documentazione prodotta dalle parti riscontri che lascino supporre qualche malfunzionamento del sistema di parte resistente durante il processo dispositivo.
6. In relazione a quanto precede, le relative contestazioni di parte attrice non possono, dunque, essere accolte.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE