

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BARTOLOMUCCI

Seduta del 06/05/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di essersi recata, in data 21/06/2025, presso un centro commerciale ove effettuava alcuni acquisti pagando alla cassa automatica con carta di credito, nel corso dei quali riceveva sul cellulare delle notifiche che la avvisavano di un prelievo di € 1.000,00.

Faceva presente che, pensando si trattasse di una clonazione, non si fosse avveduta della sottrazione del borsellino e si fosse limitata a chiamare la banca per effettuare il blocco della carta; soggiungeva, però, che – prima che il blocco venisse completato – fosse stata eseguita una seconda operazione fraudolenta per l'importo di € 1.249,00.

Sottolineava che solo il giorno successivo si fosse accorta della sottrazione del portafoglio e avesse così provveduto a sporgere denuncia.

Precisava che il codice PIN associato alla carta non fosse annotato né conservato nel portafoglio sottratto.

Chiedeva, pertanto, il rimborso delle somme fraudolentemente sottratte, oltre agli interessi legali.

Si costituiva ritualmente l'intermediario convenuto, il quale rilevava che le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere mediante lettura del microchip della carta e corretta digitazione del PIN.

Riteneva sussistente la colpa grave della cliente, in quanto il fatto che le operazioni fraudolente fossero state compiute nell'immediatezza del furto e non ci fossero stati precedenti tentativi di digitazione del PIN lasciava presumere l'incauta custodia del codice segreto congiuntamente alla carta.

Sottolineava di aver correttamente inviato due notifiche push di alert a seguito delle operazioni oggetto di controversia.

Chiedeva, pertanto, di dichiarare il rigetto del ricorso ovvero, in caso di accoglimento delle doglianze della ricorrente, di riconoscere un concorso di colpa ex art. 1227 cod. civ. e di applicare la franchigia prevista per legge.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale affermava che – diversamente da quanto affermato dalla controparte – il codice PIN fosse stato carpito durante gli acquisti effettuati presso un esercizio commerciale sito nel medesimo centro commerciale in cui, successivamente, erano state eseguite le operazioni disconosciute; aggiungeva, peraltro, che ai fini dell'esclusione della colpa rilevasse altresì l'immediato avviso alla banca per il blocco della carta.

Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale si riportava ai propri scritti difensivi.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto ad ottenere il rimborso del controvalore di una serie di operazioni di pagamento, successivamente disconosciute.

La materia, come noto, è regolata dal d. lgs. n. 11/2010 come modificato dal d. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- Payment Services Directive 2).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. strong customer authentication SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Con riferimento alla c.d. SCA gli artt. 97 e 98 della direttiva PSD2, nonché l'articolo 10-bis del d. lgs. n. 11/2010, oltre che le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea e i criteri interpretativi adottati dalla stessa Autorità (cfr. in particolare il parere dell'EBA del 21 giugno 2019), hanno stabilito che essa 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. In relazione a tutte le predette fasi, la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori, che devono essere reciprocamente indipendenti e appartenere a categorie diverse: conoscenza; inerenza; possesso.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Risulta documentalmente che le operazioni in parola consistano in un prelievo e un pagamento eseguiti in data 21.06.2025, per il complessivo importo di € 2.249,00.

Le tracciature informatiche versate in atti evidenziano che entrambe le operazioni siano state eseguite mediante lettura del chip della carta (la seconda in modalità contactless) ed inserimento del PIN; deve, concludersi, di conseguenza che esse siano state correttamente autenticate in modalità conforme a SCA, previo utilizzo dei fattori del possesso (il chip della carta) e della conoscenza (il codice PIN).

Attesa la conformità a SCA dell'operazione contestata, non resta che verificare se – dalla condotta tenuta dal ricorrente – siano evidenziabili profili di colpa grave, rispetto alla quale la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico (cfr. Coll. coord., dec. n. 22745/2019).

A tale riguardo giova rilevare che, mentre la cliente dichiara che il codice PIN associato alla carta non fosse custodito insieme alla stessa e che il codice segreto sia stato carpito dai malfattori durante gli acquisti da lei effettuati nel centro commerciale (come sarebbe confermato – secondo la sua prospettazione – dal fatto che le operazioni fraudolente sono avvenute poco dopo la sottrazione e nel medesimo centro commerciale), l'intermediario ritiene che lo strettissimo arco temporale intercorso tra l'ultima operazione autentica della cliente (11:50) e la prima operazione disconosciuta (11:59) sia tale da ritenere che il PIN fosse custodito insieme alla carta.

Inoltre, l'intermediario sostiene che, anche ammettendo che il codice segreto sia stato carpito durante l'utilizzo della carta da parte della cliente, ciò non fa venire meno la colpa grave della stessa che non ha adottato tutti gli accorgimenti necessari ad assicurare la segretezza del PIN.

A tale ultimo riguardo, il Collegio deve richiamare il consolidato orientamento di questo Arbitro, secondo cui l'eventualità che il PIN sia stato carpito durante l'utilizzo della carta non assume rilevanza, quale indice della colpa grave del cliente, in considerazione degli standard di diligenza che è ragionevole pretendere dagli utilizzatori degli strumenti pagamento.

Di contro, proprio alla luce delle allegazioni delle parti, assume rilievo assorbente proprio il ristretto arco temporale intercorrente non già dall'ora presunta del furto, bensì tra quello dell'ultima operazione legittima e la prima operazione fraudolenta: tale circostanza, infatti, appare idonea a fondare legittimamente la presunzione che i malfattori avessero a disposizione anche i codici dispositivi dello strumento di pagamento.

Sempre in relazione a tale aspetto, rileva anche la circostanza che la stessa ricorrente afferma di avere contattato l'intermediario per richiedere il blocco della carta subito dopo aver ricevuto le notifiche

relative alla prima operazione fraudolenta e che, nel corso della telefonata, sarebbe giunta anche la notifica relativa alla seconda operazione. Tuttavia ella non versa in atti il registro delle chiamate né alcun altro elemento idoneo a dimostrare quanto riferito e, in particolare, l'orario in cui detta telefonata è stata effettuata.

L'intermediario, dal canto suo, afferma di avere tempestivamente bloccato la carta producendo una schermata dalla quale si evince che il blocco dello strumento di pagamento è stato disposto alle ore 18.23; tenuto conto che la prima operazione è stata eseguita alle 17.59, mentre la seconda è stata eseguita alle 18.12 non è possibile stabilire con certezza se la telefonata di blocco sia stata effettuata tempestivamente rispetto alla ricezione della notifica push del primo pagamento fraudolento (circostanza che è l'utilizzatore a dover provare).

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE