

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) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) CESARE

Seduta del 13/01/2026

FATTO

Il cliente afferma di essere titolare del conto corrente n. 3249 e della carta di debito n. 5167***7056 presso l'intermediario convenuto. In data 20 maggio 2020 ha riferito di aver ricevuto un SMS apparentemente proveniente dall'intermediario, inserito nella chat ufficiale del mittente, con cui è stato avvisato di alcuni accessi anomali al conto. Il cliente riferisce di non aver cliccato sul link contenuto nell'SMS. Poco dopo ha scoperto che gli erano stati sottratti € 3.000,00, di cui € 2.000,00 e € 1.000,00 mediante due prelievi cardless. Il giorno stesso si è recato dai Carabinieri per sporgere denuncia e successivamente ha provveduto al formale disconoscimento delle operazioni presso l'intermediario. Data la sofisticazione della truffa e l'assenza di circostanze sospette, il cliente ritiene che debba

escludersi la sussistenza in suo capo di dolo o colpa grave. Come affermato dal Giudice di Pace di Brindisi con sentenza n. 517/2021, il furto di dati costituisce un pericolo reale del sistema bancario online e l'obbligo di fornire sicurezza nelle operazioni e tutela degli interessi dei propri correntisti, in capo all'istituto bancario, ne comporta la responsabilità in caso di operazioni autorizzate senza una preventiva verifica della certezza della legittima provenienza dell'ordine di pagamento ricevuto. Il cliente domanda il rimborso di € 3.000,00.

Nelle controdeduzioni, l'intermediario afferma che il conto corrente n. 1000/3249 risulta cointestato e sul rapporto è delegato ad operare il padre del ricorrente. Tramite servizio di home banking riconducibile al delegato, sono state disposte in data 21 maggio 2020 alle ore 11:14 e alle ore 11:17, due operazioni di prelievo cardless rispettivamente di € 2.000,00 e di € 1.000,00, successivamente disconosciute dal cliente. Alla luce degli accertamenti svolti, si è proceduto al riaddebito delle somme inizialmente accreditate. Ai clienti viene fornita, tramite sito internet, ampia informativa circa i possibili rischi di frode. Le due operazioni disconosciute sono state eseguite dopo essere state autenticate mediante ricorso a elementi di conoscenza (PIN) e di possesso (codici OTS inviati tramite SMS al numero di telefono certificato del delegato), correttamente registrate e contabilizzate, in assenza di malfunzionamenti delle procedure necessarie per la loro esecuzione. Il delegato ad operare è stato vittima di una ormai nota truffa telematica, usualmente denominata smishing/vishing, resa possibile da comportamenti gravemente colpevoli e negligenti. L'SMS con cui sarebbe iniziata la frode risulta inserito in una chat la cui intestazione differisce rispetto al canale ufficiale utilizzato abitualmente per le comunicazioni con i clienti. Detto SMS non appare nella cronologia della messaggistica istituzionale, non risulta preceduto da messaggi genuini e non presenta un contenuto attendibile, riportando un link nel quale non vi è alcun elemento riferibile ai servizi della Banca. Il delegato ha del tutto trascurato gli alert con cui è stato informato circa l'enrollment di un nuovo dispositivo alle ore 11:09 del 20 maggio 2020, rendendo così apparentemente indubbia la riconducibilità dell'operazione allo stesso. Ha anche ricevuto, sempre sul proprio numero di cellulare certificato, i codici OTS necessari per completare le singole operazioni. Non si tratta di una truffa particolarmente sofisticata, in quanto le modalità con le quali si è svolta non risultano assolutamente assimilabili all'operatività di alcun servizio della Banca. L'intermediario conclude per il rigetto del ricorso, in subordine, di riconoscere la franchigia di € 50,00.

DIRITTO

La controversia riguarda il disconoscimento di due operazioni di prelievo cardless eseguite in data 21 maggio 2020 alle ore 11:14 e 11:17 per un importo complessivo di € 3.000,00, a seguito di truffa ai danni del delegato a operare sul conto corrente cointestato del ricorrente. All'operatività contestata si applica il D.Lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II).

L'intermediario ha fornito prova dell'autenticazione delle operazioni contestate. In data 20 maggio 2020 alle ore 11:09 è stato effettuato l'enrollment di un nuovo dispositivo mediante inserimento delle credenziali statiche (USER ID e PIN) e del codice dinamico OTS inviato via SMS al numero di telefono

certificato del delegato. Il delegato ha ricevuto altresì notifica push che comunicava l'attivazione da un nuovo dispositivo, con esplicito invito a contattare la Filiale Online qualora non fosse stato lui a compiere tale operazione. Successivamente, alle ore 11:14 e 11:17, sono state disposte le due operazioni, ciascuna autorizzata mediante inserimento del PIN e del codice OTS. Le operazioni risultano autenticate mediante ricorso a un elemento di conoscenza (PIN) e a un elemento di possesso (codice OTS e device), in conformità all'autenticazione forte richiesta dalla normativa PSD2.

Una volta provata l'autenticazione, l'intermediario deve fornire la prova della colpa grave del cliente per andare esente da responsabilità.

Il ricorrente ha prodotto evidenza dell'SMS civetta inserito in una chat apparentemente riferibile alla banca. L'intermediario ha tuttavia eccepito che l'intestazione della chat differisce da quella del canale ufficiale, che il link contenuto nell'SMS non è riconducibile al proprio dominio e che nella medesima chat non sono presenti messaggi genuini. Il Collegio rileva che l'SMS civetta presenta evidenti elementi di inattendibilità che avrebbero dovuto indurre il delegato a una verifica preventiva del mittente.

Nel caso di specie, inoltre, il delegato ha ignorato la notifica push che lo avvisava dell'attivazione di un nuovo dispositivo con invito a contattare la Filiale, ha autorizzato due operazioni di importo significativo mediante inserimento dei codici OTS senza alcuna verifica nonostante il messaggio sospetto, e non ha rilevato gli elementi oggettivi di inattendibilità dell'SMS (link non riconducibile all'intermediario e assenza di messaggi genuini). Gli elementi così ricostruiti integrano la colpa grave di cui all'art. 10, comma 2, del D.Lgs. n. 11/2010.

Quanto al servizio di sms-alert, la mancata attivazione è irrilevante nelle ipotesi di più operazioni eseguite a breve distanza di tempo, in quanto la ricezione dell'alert non avrebbe potuto limitare il pregiudizio (Collegio di Coordinamento, decisione n. 8672/2024). Le due operazioni sono state infatti eseguite a distanza di soli tre minuti, tempo incompatibile con una possibile utile attivazione del cliente per il blocco dell'operazione.

Alla luce della prova dell'autenticazione delle operazioni e della colpa grave come sopra ricostruita il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE