

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) ABATE	Membro di designazione rappresentativa dei clienti

Relatore (MI) MODICA

Seduta del 28/04/2026

FATTO

Il cliente dichiara di avere ricevuto, in data 26/06/2025, un SMS che sembrava provenire dall'intermediario col quale gli veniva chiesto se avesse autorizzato un addebito di € 985,00; telefonava all'intermediario il quale lo faceva poi contattare dal Comando affinché non venissero autorizzati altri addebiti fraudolenti. Si avvedeva quindi di essere stato vittima di una truffa poiché notava di aver subito un'operazione non autorizzata pari ad € 990,00; procedeva a presentare denuncia presso le Autorità; presentava reclamo all'intermediario in data 23/10/2025, che veniva riscontrato negativamente.

Chiede la restituzione di € 990,00.

L'intermediario controdeduce che: in data 26 giugno 2025, il cliente contattava l'assistenza clienti e veniva disposto il blocco della carta; il cliente non ha fornito copia del messaggio civetta; la truffa non presentava profili di sofisticatezza; il cliente seguiva le indicazioni fornite dai sedicenti operatori e comunicava loro il codice PIN e i dati della carta di credito; successivamente il cliente avrebbe scaricato un'applicazione malevola tramite un *link* fornito dai frodatori via SMS. Segnala che le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; sussiste la colpa grave del cliente in quanto le operazioni sono state autorizzate mediante la collaborazione dello stesso con i truffatori; non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

Chiede il rigetto del ricorso.

Il cliente, nelle repliche, allega l'SMS ricevuto in cui gli si comunicava una richiesta di autorizzazione per un pagamento di € 985,00; afferma di essere stato vittima di una truffa sofisticata e aggravata; precisa che non mette in dubbio il corretto funzionamento dei sistemi informatici. Insiste nella domanda.

DIRITTO

Il cliente disconosce una operazione di pagamento mediante POS eseguita a valle di una truffa alle ore 14:33.59 del 26/06/2025 e chiede la restituzione del relativo importo, pari a € 990,00.

Dalle dichiarazioni rese dal cliente in sede di denuncia, risulta che il cliente ha fornito i dati della carta di credito e il PIN della carta su cui è stata effettuata l'operazione disconosciuta. Secondo l'orientamento unanime dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP. L'operazione va scrutinata dunque alla luce del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2). Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". L'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente" (decisione n. 22745/2019). Il Collegio, richiamati gli artt. 97 e 98 della PSD2, l'articolo 10 bis del D. Lgs. 11/2010, le 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 (in particolare il parere dell'EBA del 21 giugno 2019), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei

dati di autenticazione". L'autenticazione forte è richiesta nella fase di accesso al conto/*enrollment* dell'App/registrazione della carta sul *wallet*; nella fase di esecuzione delle singole operazioni; rispetto a qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Nel caso di specie, l'intermediario ha fornito prova di autenticazione con impiego di doppio fattore. Sulla base delle evidenze prodotte, l'operazione risulta infatti autenticata tramite utilizzo della carta fisica (elemento di possesso) e digitazione del PIN (elemento di conoscenza). L'intermediario fornisce altresì una plausibile giustificazione alla circostanza che la sede del *merchant* presso cui è stata eseguita l'operazione è Napoli, mentre il cliente si trovava a Pordenone, riconducendo la truffa al cosiddetto "*Card Relay Attack*". Si tratta di uno schema così articolato: il primo passo dell'attacco è l'invio di SMS o messaggi WhatsApp apparentemente provenienti dall'intermediario che comunicano un'attività sospetta sul conto corrente del cliente e invitano a chiamare un numero per risolvere la situazione; quando il cliente effettua la telefonata entra in contatto con un finto operatore che lo induce a fornire dati sensibili (come il numero della carta e il PIN) e lo convince ad installare un'applicazione che contiene un *malware*. Una volta che l'App viene installata, il truffatore convince l'utente ad appoggiare la propria carta di pagamento sullo *smartphone* allo scopo di eseguire una presunta verifica: in questo modo il *malware* legge i dati della carta dal *chip* NFC della stessa, inviandoli in tempo reale ai truffatori. I dati della carta di credito inviati agli attaccanti vengono usati per emulare una carta virtuale che, grazie ad una serie di accorgimenti che coinvolgono i messaggi ATR (*Answer To Reset*), viene riconosciuta come autentica dai terminali POS e dagli sportelli ATM consentendo l'esecuzione di pagamenti *contactless* e prelievi di denaro. I criminali, pertanto, riescono ad effettuare le transazioni non autorizzate su terminali POS e prelievi ATM senza dover entrare in possesso fisico della carta della vittima, purché quest'ultima abbia appoggiato la carta di pagamento al proprio *smartphone* per sfruttare così la tecnologia NFC. Le modalità con cui i truffatori entrano in possesso del PIN variano; nel caso di specie, il cliente ha dichiarato di aver comunicato direttamente il PIN della carta.

Del pari provata appare la colpa grave del cliente, vittima di una truffa banale cui avrebbe potuto sottrarsi con l'impiego di una media diligenza. Il cliente riferisce di aver ricevuto un SMS con cui gli veniva richiesto di autorizzare un pagamento pari ad € 985,00 e che avrebbe potuto chiedere informazioni chiamando il numero di cellulare ***048. Dalla documentazione versata in atti si evince che l'SMS civetta contiene errori di sintassi; il numero mittente (***174) non è riconducibile all'intermediario; il messaggio contiene riferimento all'autorizzazione di un'operazione pari a € 985,00, che non risulta dall'estratto conto; il numero ***048, da contattare per avere informazioni, non è riconducibile all'intermediario. Il cliente riferisce di avere ricevuto due chiamate dal comando dei Carabinieri alle ore 12:05 e una chiamata da Whatsapp proveniente da numero di cellulare ***800; non produce tuttavia alcuna evidenza in merito. Alla luce delle specificità del caso concreto, ritiene il Collegio che risulti provata non solo l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione nonché la sua regolarità formale, ma anche dimostrata la colpa grave di parte ricorrente (cfr. in proposito Collegio di Coordinamento, decisione n. 22745/2019), in quanto le modalità attuative delle operazioni sconosciute riflettono uno schema tipico e ormai noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, *e-mail*, SMS o altri strumenti di comunicazione, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie

credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza. Tenuto conto delle circostanze, il ricorrente deve essere considerato vittima di colpevole credulità, in quanto le modalità con le quali la truffa è stata realizzata rientrano tra quelle più diffuse e conosciute, che qualunque fruitore di servizi *on line*, dotato di normale avvedutezza e prudenza, deve essere in grado di riconoscere ed evitare (cfr. Collegio di Coordinamento n. 3498 del 26/10/2012).

La riconosciuta colpa grave del cliente, pur a fronte di operazioni accompagnate da piena prova della SCA, non esclude naturalmente che il Collegio, tenuto conto delle peculiarità della fattispecie, possa individuare altri e diversi eventuali profili di responsabilità, per esempio sul versante del rispetto degli obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius* anche *sub specie* di mancata gestione di eventi che segnalino la possibilità di frodi o anomalie; profili che, nella vicenda in esame, non ricorrono.

Sebbene le notifiche di avvenuta operazione risultino inviate alle ore 5:13 del 4/07/2025, ossia ben oltre una settimana dall'esecuzione dell'operazione fraudolenta, secondo l'orientamento dei Collegi, la mancata attivazione ovvero il mancato funzionamento del servizio di SMS-*alert* (o di servizio assimilabile) è irrilevante nelle ipotesi di esecuzione di una sola operazione di pagamento, in quanto la ricezione dell'*alert* non potrebbe limitare, in concreto, il pregiudizio dell'utente. In ogni caso, l'intermediario ha fornito evidenza di essersi prontamente attivato per contattare via telefono (senza esito) e via *mail* il cliente dopo il blocco della carta di credito. Le telefonate risultano effettuate alle ore 14:36 e 14:37, mentre la *mail* è delle ore 14:38, ossia pochi minuti dopo l'operazione; l'indirizzo mail è quello indicato dal cliente in sede di ricorso

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE