

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

La controversia trae origine dal disconoscimento di due operazioni di pagamento eseguite in data 29.03.2020 tramite i servizi di *home banking*, consistenti in una ricarica di carta e in un bonifico istantaneo, per un importo complessivo pari a € 17.351,60.

Il ricorrente espone di aver ricevuto in data 28.03.2020 un messaggio SMS apparentemente proveniente dall'intermediario, che, informandolo di un accesso anomalo al proprio conto, lo invitava ad inserire le proprie credenziali nel link riportato. Riferisce di aver ignorato la richiesta, non fidandosi. Il giorno successivo, 29.03.2020, veniva contattato telefonicamente da un soggetto che si qualificava come addetto dell'ufficio antifrode dell'intermediario e che, dimostrando di conoscere i suoi dati personali, gli comunicava di aver rilevato due bonifici sospetti effettuati il giorno precedente già bloccati e gli chiedeva se intendesse quindi confermarne o meno il blocco. Poco dopo, in coda agli altri SMS autentici precedentemente inviati dall'intermediario, riceveva un messaggio contenente il codice a sei cifre necessario per confermare il blocco delle operazioni; successivamente riceveva altri due SMS contenenti codici di sicurezza ed un messaggio che confermava l'avvenuto storno del bonifico, tutti in coda agli altri SMS precedentemente inviati dall'intermediario. Resosi conto della truffa subita e dell'indebito prelievo dal conto la somma di € 2.450,00, oltre ad ulteriori € 14.901,60, provvedeva immediatamente a bloccare sia l'applicazione di *home banking* che la propria carta di credito. In data

30.03.2020, si recava presso la propria filiale per richiedere nuovi codici di accesso al conto, i quali gli venivano inviati in coda ai messaggi truffaldini ricevuti, rendendo impossibile distinguere gli uni dagli altri e il medesimo giorno sporgeva denuncia-querela, che integrava in data 01.04.2020 e 05.05.2020. Il ricorrente conclude chiedendo, in via principale, la restituzione integrale delle somme oggetto delle operazioni contestate, assumendone la natura non autorizzata; in via subordinata, nell'ipotesi in cui il Collegio avesse ritenuto sussistenti profili di responsabilità concorrente nell'accaduto, che il danno venisse ripartito tra le parti in misura proporzionale alle rispettive responsabilità.

Nelle controdeduzioni, l'intermediario si è opposto alla domanda di rimborso, sostenendo che le operazioni disconosciute risultano correttamente autenticate, registrate e contabilizzate, senza evidenza di anomalie tecniche o di malfunzionamenti dei sistemi. Sostiene che il cliente, in denuncia, abbia affermato di aver ricevuto un SMS da lui *"ingenuamente"* ritenuto riferibile al servizio clienti, di aver aderito al link ivi riportato e di aver inserito i propri dati bancari negli spazi sottostanti della pagina apertasi, nonché di aver riferito al sedicente operatore dell'ufficio antifrode i codici pervenutigli via SMS *"senza effettivamente fare troppa attenzione agli interi testi dei due messaggi"*, rendendosi conto dello *"sbaglio fatto"* solo al termine della telefonata. Ritiene che il messaggio esca che ha dato origine alla truffa, in alcun modo a sé riferibile, sia totalmente sgrammaticato e avrebbe dovuto destare allarme in capo al ricorrente ed indurlo a chiedere chiarimenti; allo stesso modo, neppure il numero di telefono utilizzato dal sedicente operatore Antifrode gli sarebbe riconducibile. Conclude affermando che l'episodio fraudolento si è realizzato esclusivamente a causa della condotta gravemente negligente e superficiale del ricorrente e che non si tratta di truffa particolarmente sofisticata.

In sede di repliche, il ricorrente ha contestato le affermazioni dell'intermediario, non essendo corrispondente al vero che il cliente avrebbe inserito i propri dati bancari all'interno della pagina apertasi tramite link contenuto nell'SMS esca, che il messaggio esca ricevuto sarebbe stato totalmente sgrammaticato e non riconducibile alla Banca ovvero che il cliente avrebbe ignorato il contenuto dei messaggi ricevuti. Ritiene pretestuose le argomentazioni addotte dall'intermediario, preordinate esclusivamente a distogliere l'attenzione dall'impossibilità di distinguere i messaggi truffaldini dalle altre comunicazioni genuine della Banca, nonché dal fatto che il truffatore conosceva già i suoi dati anagrafici. Il cliente ha inoltre dedotto che, nel corso della medesima giornata, sarebbero stati registrati accessi ai servizi di *home banking* provenienti da indirizzi IP non riconducibili ai propri dispositivi, sostenendo che tali circostanze dimostrerebbero una carenza nei presidi di sicurezza dell'intermediario. Ha infine affermato di aver adempiuto tempestivamente agli obblighi di segnalazione e di blocco degli strumenti di pagamento non appena resosi conto dell'accaduto, ribadendo l'assenza di dolo o colpa grave nella propria condotta.

DIRITTO

Le operazioni contestate rientrano 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 PDS2, 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 in esame, risulta che in data 29.03.2020 sono state effettuate due operazioni a distanza di pochi minuti l'una dall'altra: una ricarica di carta di importo pari a € 2.450,00, eseguita alle ore 15:25, e un bonifico istantaneo di importo pari a € 14.901,60, eseguito alle ore 15:29. Tali importi coincidono con quanto richiesto in restituzione dal cliente in sede di ricorso, sebbene in sede di denuncia sia stata indicata una lieve divergenza negli importi e nella qualificazione delle singole operazioni, circostanza che non assume rilievo ai fini della presente decisione.

Dalla documentazione acquisita risulta che entrambe le operazioni sono state precedute da un accesso ai servizi di *home banking* effettuato tramite applicazione mobile, avvenuto alle ore 15:22:48 del medesimo giorno, da un indirizzo IP riconducibile all'operatività abituale del cliente e mediante il dispositivo a lui associato. Tale accesso risulta autorizzato attraverso l'inserimento di un elemento di conoscenza, costituito dal PIN, e di un elemento di possesso, rappresentato dal codice OTP generato dall'applicazione installata sul dispositivo del cliente. Pertanto, già in questa fase antecedente all'esecuzione delle operazioni, risulta integrato un sistema di autenticazione forte conforme ai requisiti previsti dalla normativa PSD2 e dalle relative norme tecniche di regolamentazione.

Con riferimento alle singole operazioni contestate, l'intermediario ha prodotto evidenze dalle quali risulta che la ricarica di carta disposta alle ore 15:25 è stata autorizzata mediante inserimento del PIN e del codice OTP generato dall'applicazione installata sul dispositivo del cliente, a seguito dell'invio di un SMS e di una notifica push contenenti indicazioni puntuali circa l'operazione da autorizzare, l'importo e lo strumento di pagamento interessato. Analogamente, il bonifico istantaneo eseguito alle ore 15:29 risulta autorizzato mediante il medesimo meccanismo di *strong customer authentication*, SCA, sempre attraverso l'utilizzo del dispositivo riconducibile al cliente e previa ricezione di messaggi di conferma recanti informazioni dettagliate sull'operazione, sul beneficiario e sull'importo.

Tali elementi consentono di ritenere adeguatamente dimostrata, da parte dell'intermediario, la corretta autenticazione, registrazione e contabilizzazione delle operazioni, secondo quanto richiesto dall'art. 10 del D.lgs. n. 11/2010.

Resta pertanto da valutare se, alla luce delle modalità concrete della vicenda, le operazioni possano comunque qualificarsi come non autorizzate ovvero se ricorrano profili di dolo o colpa grave in capo al cliente idonei a escludere il diritto al rimborso.

Dalle dichiarazioni rese dal cliente, sia in sede di denuncia sia nel corso del procedimento, emerge che egli ha comunicato telefonicamente a un soggetto terzo due codici a sei cifre di sicurezza ricevuti via SMS, necessari per l'autorizzazione delle operazioni, ammettendo di averlo fatto "*senza fare troppa attenzione agli interi testi*" dei messaggi. Tali messaggi, come risulta dalla documentazione in atti, contenevano indicazioni chiare e parlanti circa la natura dispositiva delle operazioni da autorizzare, con esplicito riferimento all'importo, alla tipologia di operazione e al beneficiario.

La vicenda si inserisce in un contesto riconducibile alle tecniche di sms *spoofing* e *vishing*, che secondo l'orientamento consolidato dei Collegi possono presentare un elevato grado di insidiosità, specie

quando i messaggi fraudolenti si inseriscono in conversazioni contenenti comunicazioni genuine dell'intermediario. Tuttavia, la valutazione della colpa grave dell'utilizzatore non può fondarsi su automatismi, dovendo essere condotta caso per caso alla luce di tutte le circostanze concrete.

Nel caso in esame, accanto alla presenza di messaggio civetta caratterizzato da link non riconducibile all'intermediario - che il ricorrente dichiara di aver cliccato, sia pure negando aver inserito i propri dati bancari - e da grossolani errori grammaticali, nonché di ulteriori messaggi truffaldini che presentano alcuni errori grammaticali, sintattici e di punteggiatura, anche di storno, risultano pervenuti al cliente messaggi "parlanti" di conferma delle operazioni, successivi e autonomi rispetto agli altri, idonei a richiamare l'attenzione dell'utilizzatore sull'effettiva autorizzazione di specifiche operazioni di pagamento. La comunicazione e la conferma di tali codici, destinati a rimanere strettamente riservati, costituisce una violazione degli obblighi di custodia e di diligente utilizzo dello strumento di pagamento posti a carico dell'utilizzatore dall'art. 7 del D.lgs. n. 11/2010.

Rispetto alla telefonata ricevuta dal sedicente operatore, dalle evidenze prodotte risulta che tale chiamata non è riconducibile all'intermediario, mentre all'interno del registro telefonico sono presenti chiamate effettivamente riferibili all'intermediario.

Le deduzioni del cliente circa la presenza di accessi provenienti da indirizzi IP diversi da quelli abitualmente utilizzati non risultano sufficienti a superare il quadro probatorio complessivo, atteso che le operazioni contestate risultano comunque eseguite mediante il dispositivo a lui associato e previa autenticazione forte. Parimenti, la circostanza che il cliente abbia provveduto tempestivamente al blocco degli strumenti di pagamento una volta resosi conto dell'accaduto, non incide sulla valutazione della condotta tenuta nella fase antecedente e contestuale all'esecuzione delle operazioni.

Alla luce di quanto precede, deve ritenersi che l'intermediario abbia assolto all'onere di dimostrare la corretta autenticazione delle operazioni e che l'evento dannoso sia riconducibile a una condotta gravemente negligente del cliente, consistente nella comunicazione a terzi dei codici di sicurezza necessari per l'autorizzazione delle operazioni, nonostante il contenuto chiaro dei messaggi ricevuti. Ne consegue che le operazioni non possono qualificarsi come non autorizzate ai sensi della normativa applicabile e che non sussistono i presupposti per l'accoglimento della domanda restitutoria.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE