

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) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) FORMAGGIA

Seduta del 17/03/2026

FATTO

Il ricorrente, nel ricorso, integrato per completezza con quanto ricostruito nel reclamo, afferma che in data 31/10/2024 riceveva un primo SMS da un'utenza che si qualificava come la propria banca, e che informava di un accesso all'APP di banca da altro dispositivo; che il messaggio non veniva aperto; che nessuna iniziativa a tutela del cliente veniva messa in atto dalla banca dopo questo primo tentativo di truffa; che alle ore 08:04 del 04.11.2024 il ricorrente riceveva un altro SMS, con cui gli veniva comunicato di un presunto accesso anomalo all'app di banca da altro dispositivo e della necessità di cliccare su un link fornito per bloccare l'asserito accesso; che il ricorrente cliccava quindi sul link ed entrava nel sito web che riconosceva essere quello della banca, ove gli veniva chiesto l'inserimento del codice cliente, del quale egli era però sprovvisto; che dunque la schermata veniva chiusa senza completare alcuna procedura; che a questo punto il ricorrente riceveva una chiamata telefonica dal numero 02*****01, nel corso della quale l'interlocutore, qualificatosi come addetto alla sicurezza della banca, dimostrava di essere in possesso dei dati suoi personali e bancari; che il sedicente operatore di banca insisteva affinché il cliente procedesse al disconoscimento di una presunta operazione di acquisto fraudolenta cliccando nuovamente sul link inviato, richiesta che questi eseguiva; che quando però l'interlocutore aggiungeva una richiesta di creazione di una carta virtuale, il ricorrente, insospettito, interrompeva la chiamata; che tentava allora più volte di contattare il proprio referente di banca senza successo; che provvedeva quindi a modificare il codice di accesso all'app di home banking; che solo dopo 5 tentativi di chiamata riusciva a contattare gli operatori al numero di assistenza della banca, i quali gli comunicavano un avvenuto prelievo dalla carta di credito n.53*****55, di € 2.375,50; che

bloccava dunque la carta e seguiva le indicazioni dell'operatore di banca, il quale lo invitava ad attendere la contabilizzazione del pagamento; che per questa ragione aveva presentato denuncia e formale disconoscimento solo dopo 4 giorni dal verificarsi dei fatti; che sussisteva una responsabilità della banca, tenuta a garantire il corretto funzionamento del sistema di sicurezza e a provare la colpa grave del cliente, al quale non spetta dimostrare la diligente custodia delle proprie credenziali.

Chiede la restituzione della somma di € 2.375,50 per il prelievo illecito subito in data 4.11.2024 a seguito di truffa, il riconoscimento del risarcimento pari ad € 500,00 per il disagio recato e la liquidazione dei compensi per l'intervento professionale per € 500,00 oltre oneri accessori, con riserva di ogni ulteriore richiesta di ristoro per i danni patiti e *patiendi*.

L'intermediario, nelle controdeduzioni depositate, sottolinea che il cliente è titolare della carta di credito n. 53*****55, legata al conto corrente n. 7*****87, abilitata all'internet banking, con cui è stata eseguita l'operazione oggetto di controversia; che la banca garantisce un servizio Internet banking con inserimento simultaneo di password statiche (in questo caso: codice titolare e codice PIN) e dinamiche (in questo caso: codice O-Key); che la banca fornisce alla propria clientela ampia informativa in ordine alla prevenzione delle frodi informatiche nella sezione "Sicurezza" del proprio sito; che l'operazione di pagamento in contestazione, così come la precedente operazione di variazione dei limiti operativi della carta, risulta approvata correttamente tramite un sistema di autenticazione forte e senza alcun malfunzionamento o compromissione dei sistemi, nel rispetto dei requisiti SCA; che l'episodio fraudolento è imputabile esclusivamente alla negligenza del cliente, la cui colpa grave emerge dal fatto che non si tratta di una truffa particolarmente sofisticata, che il cliente non ha allegato il primo SMS ricevuto (il 31.10.2024), che l'SMS civetta del 4.11.2024 proviene da un numero non riferibile alla Banca; che lo smartphone del cliente segnala automaticamente il rischio di smishing/phishing nella chat, inoltre, il link, cliccato dal cliente, ha un dominio non italiano (spagnolo ".es") privo di riferimenti alla banca; che il Cliente ha ammesso di aver seguito le istruzioni ricevute per disconoscere il presunto acquisto online fraudolento; che dai LOG prodotti emerge che il cliente aveva aumentato i limiti operativi e autorizzato un pagamento di € 2.375,50 presso B*****m.; che, inoltre, il messaggio inviato dalla banca per autenticare l'operazione era esplicito nell'indicare l'autorizzazione di un pagamento presso l'*e-commerce* in questione, circostanza incompatibile con un presunto "storno"; che nel modulo di disconoscimento, il ricorrente conferma di aver disposto personalmente le operazioni su sollecitazione di soggetti sconosciuti; che il cliente avrebbe avuto il tempo sufficiente per contattare la Banca ed effettuare le dovute verifiche, specie se si considera che questi fin da subito aveva colto elementi di anomalia nelle comunicazioni; che, quanto al richiesto rimborso delle spese legali, il ricorrente non aveva prodotto alcuna documentazione relativa agli esborsi, e comunque la scelta di avvalersi di un legale è discrezionale e non richiesta per le pratiche ABF, sicché è da escludere la ripetibilità.

Conclude chiedendo, in via principale, di dichiarare inaccoglibile in quanto immotivata ed infondata, la richiesta restitutoria della ricorrente, e, in subordine, denegatamente, ove si ravvisassero profili di responsabilità in capo all'intermediario convenuto, di definire la ripartizione fra le parti del danno in misura proporzionale alle rispettive effettive responsabilità ai sensi dell'art.1227 c 1 e 2 c.c.

Il ricorrente in sede di repliche, contesta quanto affermato dall'intermediario negando di aver effettuato l'accesso al servizio di internet banking, di aver inserito o fornito il codice titolare né il codice PIN, di aver autorizzato la variazione dei limiti operativi della carta di debito, di aver inserito i codici OTP, operazioni fatte invero dal sedicente operatore bancario; contesta, ancora, l'allegazione dell'intermediario rispetto alla non particolare complessità della truffa, alla mancata attivazione del cliente, il quale invece aveva tentato svariate volte senza successo di contattare l'assistenza della banca dalle 9:30 alle 10:30; che i malfattori conoscevano le coordinate di entrambe le carte del cliente ed i suoi dati anagrafici; sostiene che la banca non aveva provato di aver garantito sistemi idonei ad impedire nel concreto la truffa in oggetto; afferma che il ricorso alla difesa tecnica del cliente era legittimo e necessario a fronte del rigetto del disconoscimento, della complessità delle questioni trattate, dell'entità della somma.

L'intermediario, nelle controrepliche, rileva che quanto affermato dalla controparte era smentito dai LOG prodotti, e, richiama le difese e conclusioni rassegnate.

DIRITTO

In fatto si osserva che oggetto del ricorso è una sola operazione disconosciuta, relativa ad un acquisto *online*, eseguita il 04/11/2024 alle ore 09:26, dell'importo di € 2375,50.

L'operazione è stata eseguita con la carta di credito del cliente in *e-commerce*, mediante circuito 3DS e pertanto direttamente dal sito internet del *merchant*.

È in atti la denuncia del cliente presentata in data 08/11/2024, ove questi descrive la truffa nei medesimi termini del ricorso e del dettagliato reclamo.

In diritto si osserva che alla data delle operazioni trovava applicazione 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), entrato in vigore il 13/01/2018.

Con riferimento alla *strong customer authentication* (cd. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PSD2, 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. (Per un elenco esemplificativo dei fattori di autenticazione *compliant* con la PSD2, cfr. Opinion EBA del 21 giugno 2019).

Dalle dichiarazioni rese dal cliente nel ricorso e nel reclamo risulta che il cliente aveva cliccato sul link ricevuto mentre parlava al telefono con il sedicente operatore bancario; ciò sembra indicativo del fatto che l'operazione sia stata da lui posta in essere direttamente. Tuttavia il cliente nega di aver disposto o autorizzato alcuna operazione di variazione dei limiti operativi o di pagamento. Ciò induce a ritenere, invece, sussistente un concorso causale dell'utente in fase dispositiva o autorizzativa. In questo caso, deve tenersi conto del consolidato orientamento dei Collegi secondo cui, 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. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.Lgs. 11/2010.

Pertanto, si ritiene di procedere all'esame sulla prova della sussistenza della SCA ai sensi del D.Lgs. 11/2010.

L'intermediario fornisce tracciature informatiche-LOG ed altre evidenze e, negli atti, si riporta al loro contenuto, dandone sostanzialmente una spiegazione.

A questo proposito si rammentano i principi generali espressi dai collegi in merito alla valenza da attribuire alle informazioni presenti nei *log* prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di pagamento disconosciute (artt. 10, comma 1 e 10-bis del D.lgs. 11/2010), nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza). Tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di

autenticazione forte, i collegi ritengono che, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP (Prestatore dei Servizi di Pagamento) nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione.

I collegi ritengono inoltre che eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c..

Sulla base di tali principi consolidati nell'orientamento dei collegi, vanno esaminate le evidenze emergenti dalle tracciature informatiche e dagli argomenti esplicativi forniti dall'intermediario con riguardo alle varie fasi attraverso le quali si sono estrinsecate le operazioni qui contestate.

Nel caso in esame, si ritengono rilevanti le evidenze emergenti in particolare dagli all.9, 11, 12 prodotti dall'intermediario, che danno conferma alle sue deduzioni.

Questi premette che il cliente accede al proprio home banking prevalentemente da web browser o da APP, usando un dispositivo identificato con il codice fd7*****218. Ricostruisce quindi l'operatività fraudolenta partendo da un precedente accesso, alle ore 9.14 del 4.11.42024, all'*home banking* da web browser, seguito da una operazione di variazione dei limiti operativi di una carta di debito (n.51*****457) intestata al cliente, diversa dalla carta di credito (n. 53*****55) con cui poi è stata posta in essere l'operazione contestata. Richiama in proposito l'all.9, da cui si ha evidenza che, relativamente a tale accesso, la prova della SCA è data da un primo fattore di autenticazione rappresentato dal possesso del dispositivo fd7*****218 a cui arriva la PUSH validata con OTP, e da un secondo fattore di autenticazione rappresentato dalla conoscenza del codice PIN e del "codice titolare" inizialmente inseriti per accedere, così come del PIN successivamente inserito per validare la PUSH di OTP "authType:PIN".

In effetti, benché la variazione dei limiti operativi ha riguardato la carta di debito suddetta, mentre l'operazione di pagamento disconosciuta è stata effettuata con la distinta carta di credito suddetta, e quindi sono stati utilizzati due strumenti di pagamento diversi, il breve spazio temporale di soli pochi minuti tra le due operazioni le fa ritenere avvenute nella stessa sessione, e quindi qualificare come funzionalmente collegate.

Per la seconda vi è evidenza del corretto inserimento del codice OTS inviato via SMS al dispositivo del cliente, quale fattore di autenticazione rappresentato dal possesso. Non è qui necessaria, per ritenere sussistente la SCA, la presenza anche di un ulteriore fattore di autenticazione, proprio perché tale operazione appare funzionalmente collegata ed è stata eseguita a distanza così ravvicinata (alle ore 9.18) da rientrare nell'ambito della stessa sessione di accesso a Web Browser (delle ore 9:14) precedentemente analizzata e perfezionatasi, come rilevato, con la SCA con doppio fattore. Si ricorda infatti che in tema di riutilizzo di un fattore già utilizzato in fase di accesso all'APP, la Q&A 2018_4141 dell'EBA afferma che uno degli elementi utilizzati per il login può essere riutilizzato a condizione che l'altro elemento della SCA venga eseguito al momento dell'avvio del pagamento e che l'elemento di collegamento dinamico richiesto dall'art. 97 PSD2 (per transazioni di pagamento a distanza) sia presente e collegato a quest'ultimo elemento. Seppure il riferimento dell'EBA sia relativo alla validità del riutilizzo di uno dei fattori SCA per l'autenticazione di una successiva operazione di pagamento, si ritiene applicabile la linea guida anche nel caso di specie, caratterizzato da analoga situazione.

Con riferimento, dunque, all'operazione contestata, l'intermediario afferma che l'operazione di pagamento, effettuata *online* con la carta di credito n. 53*****55, è stata autenticata tramite inserimento del codice OTP recapitato a mezzo SMS al telefono/SIM del cliente sul sito dell'esercente (fattore di possesso), previo inserimento delle credenziali statiche date dal numero della carta di debito e dal codice CVV.

Dal complesso delle evidenze prodotte si ricava che in effetti l'operazione è avvenuta in modalità 3DS, senza digitazione del PIN ("uso PIN=0"), autenticata con inserimento del codice OTS ricevuto tramite SMS al numero +393*****5, riferibile al numero di telefono del cliente come fornito in sede di

denuncia, ed inserimento dei dati della carta tra cui il CVV ("uso CVV = 1"). È dubbio che l'inserimento del CVV e dei dati della carta possa costituire un elemento di possesso ai fini della SCA, ma in ogni caso può essere riutilizzato il fattore dell'operazione precedente proprio perché il ravvicinato spazio temporale e il collegamento funzionale consentono di qualificare i passaggi come avvenuti nella stessa sessione.

Per tutto quanto osservato, deve ritenersi assolto l'onere probatorio a carico dell'intermediario sulla sussistenza della SCA.

Appurata la dimostrazione della SCA da parte dell'intermediario, si deve considerare la condotta delle parti e i profili rilevanti per la valutazione di sussistenza della colpa.

In proposito si premette che non è configurabile una responsabilità oggettiva a carico dell'intermediario, sicché spetta al Collegio verificare se, in concreto, vi sia stata una responsabilità concorrente del PSP secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode (quali ad esempio, la mancanza o temporanea indisponibilità del numero verde del PSP, o il mancato rilievo di indici di frode).

Nel caso in esame, dalle evidenze prodotte si ricava che il numero con cui è avvenuto il contatto non è riconducibile all'intermediario; che dei messaggi riferiti dal ricorrente non vi è evidenza; che lo smartphone del cliente segnala automaticamente il rischio di *smishing/phishing* nella chat; che il link cliccato dal cliente ha un dominio non italiano (spagnolo ".es") ed è privo di riferimenti alla Banca; che la chiamata che il cliente assume di aver ricevuto dopo la ricezione dell'SMS civetta è effettivamente da un numero riconducibile al servizio *SOS carte*; che il cliente allega in merito (all.3) evidenze del registro chiamate da cui risulta che il numero è quello indicato sul sito web dell'intermediario per lo specifico servizio di blocco carte, presente alla sezione "SOS carte: il numero ISP da memorizzare"; che la banca prescrive al cliente di memorizzare il numero e di trascriverlo su un foglietto da custodire nel portafoglio; che non vi sono evidenze relative al blocco della carta che il cliente assume di aver chiesto; che il cliente non contesta il superamento del plafond di spesa e, non avendo prodotto il contratto, non è possibile stabilire i limiti operativi eventualmente previsti; che non vi è evidenza di *alert*, ma, la mancata attivazione o il mancato funzionamento del servizio di *sms-alert* (o di servizio assimilabile) è irrilevante nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'*alert* non potrebbe limitare, in concreto, il pregiudizio dell'utente; che non emergono indici di anomalia o di frode rilevabili dall'intermediario a fronte peraltro di una contestazione riguardante una sola operazione compiuta.

Nel complesso, quindi, non si riscontrano elementi tali da poter configurare a carico dell'intermediario una condotta colposa che abbia potuto avere una correlazione causale alla realizzazione della frode ai danni del cliente.

Tutto quanto rilevato comporta il rigetto del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE