

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 14/01/2026

FATTO

Con ricorso dell'11.9.2025, parte attrice riferisce di aver ricevuto, in data 4.8.2025, sull'*email* della piattaforma (...) un messaggio con il quale V.B. comunicava di avere acquistato l'ipad che il ricorrente aveva messo in vendita. Con l'occasione, il mittente trasmetteva un allegato con il quale invitava il ricorrente ad aprire un *link* per convalidare la vendita; di aver cliccato sul predetto *link*, non avendo mai eseguito transazioni di vendita in quel sito. Veniva quindi indirizzato su un'altra pagina con il *login* [della piattaforma] nella quale avrebbe dovuto inserire i dati della carta di debito ***9946; di avere chiesto chiarimenti tramite la *chat* presente sulla pagina della transazione; di aver ricevuto rassicurazioni in merito ad eventuali truffe dal contatto con E*** [assistenza della piattaforma]; di avere inserito i dati richiesti; di aver ricevuto subito dopo una notifica sul proprio telefono cellulare con la quale veniva informato dell'esecuzione di un addebito sul proprio conto per € 495,00; di avere subito contattato a mezzo telefono l'assistenza della banca e di avere bloccato la carta di debito.

In sede di controdeduzioni, l'intermediario eccepisce che, a seguito dell'inserzione sul sito [della piattaforma], realizzata dal ricorrente per effettuare la vendita di un bene di sua proprietà, effettuava in data 4.8.2025, in favore di [intermediario], un pagamento di € 495,00 con la carta di pagamento ***9946, addebitato sul conto corrente a lui intestato; in data 11.8.2025, egli disconosceva il citato pagamento, sottoscrivendo l'apposito modulo nel quale dichiarava di aver eseguito l'operazione in seguito alla vendita di un bene attraverso il sito [della piattaforma], seguendo le istruzioni a lui fornite per l'incasso della somma; in pari data, presentava denuncia presso la Questura di Roma. La banca non aveva accolto la richiesta di rimborso, dato che l'operazione risulta effettuata con le credenziali del

cliente. Aveva fatto seguito un ulteriore reclamo, che la banca aveva riscontrato negativamente in data 10.9.2025. Quanto esposto dimostra che la vicenda si è svolta senza il coinvolgimento dei sistemi informatici né del personale della banca, che pertanto risulta esente da qualsiasi profilo di responsabilità. È evidente che il ricorrente al momento di registrare la carta, sulla scorta delle istruzioni del sedicente acquirente, ha effettuato l'operazione di pagamento nell'erronea convinzione che essa avrebbe portato ad un accredito, e non un addebito, in suo favore; di conseguenza, la banca ha eseguito l'ordine di pagamento conformemente alle istruzioni impartite dal cliente; l'operazione di pagamento è stata effettuata dal ricorrente, nonostante le chiare informazioni contenute nel messaggio *push* da lui ricevuto, a seguito del quale egli autorizzava l'operazione.

In sede di repliche, parte ricorrente riferisce che, il 4.8.2025, nell'ambito di una trattativa per la vendita di un bene pubblicato sul sito [della piattaforma], è stato indotto in errore da un soggetto che si presentava come acquirente. Seguendo le istruzioni ricevute tramite *chat* della piattaforma, ha cliccato su un *link* apparentemente riconducibile [alla piattaforma], per "verificare la carta" in vista dell'accredito della somma pattuita. Successivamente, ha ricevuto una notifica *push* sull'*app* dell'intermediario, priva di indicazione dell'importo, che riportava un messaggio simile a quello di una verifica bancaria di € 0,00. Convinto si trattasse di una procedura di sicurezza per la ricezione del pagamento, il ricorrente ha accettato la notifica di € 0, senza rendersi conto che essa avrebbe autorizzato un trasferimento di denaro di € 495,00 verso [intermediario]. Il consenso, pertanto, è viziato da errore essenziale e indotto da raggiro, e come tale non può produrre effetti giuridici.

La notifica *push* ricevuta non riportava l'importo dell'operazione, non indicava il beneficiario né la causale, e risultava identica alle notifiche di sicurezza comunemente inviate dalla banca per semplici verifiche di pagamento. Tale modalità non consente al cliente di rendere un consenso informato, contravvenendo ai principi di chiarezza e sicurezza previsti dagli artt. 7 e 8 del d.lgs. n. 11/2010. L'intermediario, pur essendo a conoscenza dell'aumento di truffe legate a falsi *link*, non ha predisposto misure preventive adeguate: nessun *alert* antifrode è stato attivato, nonostante la natura atipica dell'operazione; non è stata verificata la coerenza del destinatario con le operazioni usuali del cliente e non è stato impedito il pagamento nonostante la segnalazione di disconoscimento entro pochissimi giorni.

In sede di controrepliche, l'intermediario, nel confermare quanto rappresentato in occasione delle controdeduzioni, precisa che nel modulo di disconoscimento il cliente ammette di avere registrato la sua carta di pagamento su un sito che pareva riconducibile [alla piattaforma]. La Banca ha eseguito l'operazione conformemente alle istruzioni impartite dal cliente, senza che possa esserle imputata alcuna responsabilità. L'autorizzazione della transazione risulta confermata dalle tracciate informatiche. Le contestazioni sollevate dal cliente in merito alla presunta scarsa chiarezza del messaggio *push* non trovano riscontro: il contenuto del messaggio, come documentato agli atti, è inequivocabile. Nessun obbligo di monitoraggio preventivo dell'operatività dei clienti è posto in capo alla banca, come più volte sostenuto dalla giurisprudenza della giustizia ordinaria e dell'ABF.

In relazione alle rispettive argomentazioni, il ricorrente conclude, dinanzi all'Arbitro, che «nel mio caso non vi è stato dolo, in quanto non ho tratto alcun vantaggio dall'operazione; non vi è stata colpa grave, poiché ho agito con prudenza, seguendo solo indicazioni apparentemente legittime fornite dal portale e dalla presunta assistente [della piattaforma]. Ad oggi la prova non è stata fornita. A causa di questa frode ho subito una perdita economica immediata di € 495,00; disagio e preoccupazione legati al blocco delle carte e alla necessità di verificare costantemente la sicurezza del conto. Chiedo che l'ABF voglia accogliere il presente ricorso e ordinare alla banca il rimborso integrale di € 495,00; il riconoscimento della mia condotta diligente ed escludere ogni responsabilità personale». Dal canto suo, l'intermediario chiede al Collegio di «dichiarare inaccoglibile il ricorso in quanto del tutto infondato in fatto ed in diritto».

DIRITTO

La controversia ha ad oggetto il disconoscimento di una transazione *e-commerce* di € 495,00, eseguita il 4.8.2025. La banca afferma che dalle verifiche completate è emerso che nel momento in cui risultano effettuate le operazioni disconosciute le infrastrutture tecnologiche dell'intermediario non presentavano anomalie o malfunzionamenti e che le stesse sono state eseguite in modalità di commercio elettronico sicuro e autorizzate mediante il servizio a distanza con le credenziali esclusivamente affidate al ricorrente (codici statici e dinamici). L'intermediario ha prodotto la tracciatura dalla quale risulta che l'operazione è stata effettuata nonostante le chiare informazioni contenute nel messaggio *push* ricevuto dal ricorrente sul proprio *device* (fattore di possesso) e valorizzata con fattore di conoscenza/inerenza in data 4.8.2025 ("Stai autorizzando il pagamento di 495.00 EUR presso (...) del 4.8.2025 17:16 con la carta 539768xxxxxx9946"). L'operazione di pagamento è stata autorizzata direttamente dal ricorrente mediante il dispositivo utilizzato abitualmente dallo stesso e non si è verificato nessun indice di criticità e/o anomalia.

Parte ricorrente afferma di aver ricevuto via portale della piattaforma una *email* apparentemente proveniente dalla piattaforma stessa, con la quale veniva informato dell'acquisto, da parte di un terzo sconosciuto, dell'Ipad messo in vendita. Nella stessa *email*, parte ricorrente veniva invitata ad aprire un *link*, azione necessaria per convalidare la vendita effettuata. Dopo aver cliccato nel *link*, parte ricorrente veniva indirizzata ad una pagina con i loghi della piattaforma, nella quale ha inserito i dati della propria carta di pagamento collegata al conto corrente. Prima dell'inserimento dei dati aveva chiesto chiarimenti sulla *chat* presente sulla pagina della transazione. In particolare, dopo aver cliccato sul punto interrogativo, si è messo in contatto con E*** dell'assistenza della piattaforma, dalla quale ha ricevuto rassicurazioni sulla legittimità dell'operazione. Ha poi ricevuto la notifica sul proprio cellulare dell'avvenuto addebito. Immediatamente ha contattato via filo l'assistenza dell'intermediario e bloccato la carta. In generale, laddove il ricorrente ammetta (come nel caso di specie) di aver dato seguito a una comunicazione di *phishing* (via *mail*, *sms*, o chiamata vocale), i Collegi, in linea con la decisione n. 3498/2012 del Collegio di coordinamento, ritengono che il cliente sia vittima di colpevole credulità, risultando tali forme di accalappiamento ormai note al pur non espertissimo navigatore di internet. Così, del resto, ha deciso il Collegio di Roma in un caso analogo, con decisione n. 1672 del 27.2.2024: «in particolare, il *phishing* operato tramite semplice *email* o *sms* (chiamato, in quest'ultimo caso, *smishing*) viene ritenuto fenomeno ormai diffusamente noto, che qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso dell'*home banking*, dovrebbe conoscere. Dalla documentazione versata in atti, il Collegio rileva come nel caso di specie l'intrusione non autorizzata nel sistema - lungi dall'essere causata da un insufficiente grado di protezione informatica del servizio offerto dall'intermediario - appare ascrivibile a colpa grave della cliente, incappata, per l'appunto, in un caso di *phishing* con conseguente utilizzo abusivo delle sue credenziali di accesso. Ed, infatti, la stessa ricorrente sostanzialmente ammette di aver dato seguito alle istruzioni contenute nel messaggio ricevuto sulla propria posta elettronica, che erroneamente credeva genuino. Come rilevato dal Collegio di Coordinamento (decisione n. 1820/2013), nell'ipotesi del *phishing*, "il cliente è vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di accalappiamento possono dirsi ormai note al pur non espertissimo navigatore di *internet*».

Nel caso di specie, il ricorrente ha instaurato le trattative per la vendita di un bene su un sito *internet* non riconducibile al resistente, che quindi non è stato coinvolto nella truffa né può, tanto meno, risponderne. Nello stesso senso cfr. Collegio di Roma, decisione n. 6534 del 4.6.2024.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE