



COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) BULLO	Membro designato dalla Banca d'Italia
(BO) LUCARELLI	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore LORENZA BULLO

Seduta del 20/10/2025

FATTO

Parte ricorrente espone quanto segue:

- in data 3/03/2025, visionando l'estratto conto, si avvedeva della presenza di alcuni addebiti relativi ad operazioni eseguite mediante la sua carta;
- in particolare, risultavano n. 3 *pagamenti online rispettivamente di € 990,00, € 990,00 e € 490,00, oltre a un bonifico di € 2.490,00*;
- nega di aver mai eseguito tali operazioni;
- non ha smarrito né subito il furto della sua carta, che è ancora in suo possesso;
- in data 1/03/2025 la banca le aveva comunicato a mezzo mail di cambiare il Bancomat, invitandola a recarsi presso la filiale per la sostituzione della carta;
- la nuova carta prevedeva massimali più elevati rispetto alla precedente;
- applicando i massimali relativi alla carta precedente il danno sarebbe stato nettamente inferiore.

Parte ricorrente, esperito il reclamo a seguito del quale ha ottenuto un rimborso solo parziale (limitato al bonifico disconosciuto) chiede all'Arbitro di condannare l'intermediario convenuto al rimborso delle residue somme fraudolentemente sottratte dai malfattori mediante *tre pagamenti POS con carta bancomat* (euro 990,00, più euro 990,00, più euro 490,00), per un totale complessivo chiesto a

rimborso di euro 2.470,00; contestualmente riconosce che il bonifico non autorizzato di euro 2.490,00 eseguito nella stessa giornata del 3.3.25 dai truffatori le è stato restituito dall'intermediario.

L'intermediario resiste alla pretesa contro deducendo quanto segue:

- le operazioni contestate sono state autorizzate mediante lettura del chip della carta e digitazione del codice PIN;
- di aver inviato un alert alla cliente dopo ciascun pagamento;
- la cliente nella denuncia e nel modulo di segnalazione di operazioni fraudolente si è limitata a disconoscere le operazioni;
- in data 17/03/2025 ha presentato un ulteriore modulo di disconoscimento nel quale ha precisato che *"in data 2 marzo 2025 – giorno precedente a quello in cui sono state disposte le operazioni disconosciute – ho eseguito un pagamento on-line di euro 29,00 a favore di h* con il mio bancomat visa debit n. *91. Ma non mi è mai arrivata la conferma di questo pagamento da parte del beneficiario. Il giorno successivo, dopo essermi accorta delle operazioni pos eseguite fraudolente, mi sono ritrovata con il cellulare rallentato e bloccato non potendolo più utilizzare e nemmeno spegnere. Come se mi fosse stata installata un'applicazione o malware o virus che non mi permetteva più l'utilizzo ed emetteva uno strano suono"*;
- la Banca in precedenza collocava Carte di Debito U* emesse da un altro intermediario e aveva tempestivamente comunicato alla Clientela che dal 1/03/2025 tali carte di debito non sarebbero state più operative;
- i Clienti che hanno deciso di continuare a utilizzare una carta bancomat collegata al proprio conto corrente, hanno, tempo per tempo, preso contatto con la propria Filiale di riferimento per valutare la contrattualizzazione della Carta Visa Debit, su base volontaria;
- la ricorrente in data 23/01/2025 ha richiesto l'emissione di una carta Visa Debit *mantenendo i massimali standard della stessa che prevedono, di default, un Massimale Giornaliero di pagamento POS di € 2.500*;
- la decisione di mantenere i massimali proposti di default o, al contrario, di richiederne la riduzione o l'aumento, è lasciata all'autonomia del cliente; la ricorrente non ha mai richiesto la riduzione di massimali;
- dopo aver utilizzato in modo fraudolento la carta bancomat della ricorrente, i malviventi hanno avuto accesso anche alla sua home banking tramite inserimento di UserID, password e del codice OTP ricevuto tramite SMS ovvero notifica PUSH in app;
- tale circostanza è stata resa possibile dal comportamento gravemente negligente della ricorrente che ha messo a disposizione dei malfattori tutti gli strumenti necessari per dare esecuzione alla frode;
- il sistema antifrode della banca ha impedito l'esecuzione di n. 2 operazioni di ricarica cellulari di € 100,00 ciascuna e n. 2 bonifici istantanei di € 990,00 ciascuno, limitando in modo rilevante il danno occorso alla cliente;
- è invece stata eseguita una operazione di bonifico di € 2.490,00, che tuttavia è già stata rimborsata alla cliente.

L'intermediario conclude pertanto per il rigetto del ricorso, stante da un lato la diligenza della Banca e dall'altro la partecipazione attiva e determinante della ricorrente ad eventi che si pongono al di là dello sforzo diligente richiesto dalla banca stessa.

DIRITTO

Il ricorso ha ad oggetto la richiesta di rimborso di tre operazioni disconosciute costituite da tre pagamenti POS (i primi due per euro 990,00 ciascuno, mentre il terzo per euro 490,00), pagamenti tutti eseguiti in data 3.3.2025 nell'arco di due minuti tra le 14.56 e le 14.57 con la medesima carta di debito, per un importo complessivo chiesto a rimborso di euro 2470,00.

A supporto della richiesta parte ricorrente ha allegato denuncia alla PS presentata il 5.3.2025 dalla quale si evincono date, ora e importi degli addebiti sulla carta di debito utilizzata, elementi che coincidono con la documentazione depositata dall'intermediario (modulo disconoscimento e lista movimenti carta) .

Alla luce delle informazioni e della documentazione acquisita, le operazioni per cui è ricorso possono essere così sintetizzate:

DATA	ORA	TIPOLOGIA	ESEGUITA	IMPORTO
3/03/2025	14.56	Pagamento POS	SI	€ 990,00
3/03/2025	14:56	Pagamento POS	SI	€ 990,00
3/03/2025	14:57	Pagamento POS	SI	€ 490,00

Non constano informazioni relative al blocco dello strumento di pagamento.

Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Dalla richiamata normativa e, in particolare, dall'art. 10 del d. lgs. 11/2010, discende che, qualora l'utilizzatore neghi - come nella vicenda in esame - di aver autorizzato le operazioni di pagamento in oggetto, gravi sull'intermediario l'onere di provare l'avvenuta autenticazione delle medesime operazioni, la loro corretta registrazione e contabilizzazione, nonché il mancato verificarsi di malfunzionamenti delle procedure necessarie per la loro esecuzione o di altri inconvenienti. Tale prova –precisa il comma 2 del citato articolo- non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi sul medesimo gravanti, essendo onere del prestatore di servizi di pagamento fornire anche la prova della frode, del dolo o della

colpa grave dell'utente. Nel caso di mancato assolvimento dell'onere probatorio di cui sopra, l'intermediario è obbligato a riaccreditare l'importo delle operazioni sul conto del cliente, ai sensi dell'art. 11 del medesimo d.lgs. n. 11/2010.

L'onere di dimostrare la colpa grave o il comportamento fraudolento del titolare dello strumento di pagamento grava pertanto sull'intermediario, ma, come più volte affermato dai Collegi territoriali e dal Collegio di Coordinamento, la relativa prova può essere fornita mediante «indizi chiari, precisi e concordanti idonei a comprovare che parte ricorrente non abbia custodito la carta di pagamento con la dovuta diligenza» (cfr. la decisione ABF, Collegio di coordinamento, n. 897/2014), ovvero, fermo restando che «la produzione documentale volta a provare l'«autenticazione» e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio», essere fornita dall'intermediario indicando «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» (così la decisione ABF, Collegio di Coordinamento, n. 22745/2019).

Il prestatore di servizi di pagamento deve prevedere forme di autenticazione c.d. «forte» per l'autorizzazione di operazioni di pagamento a tutela della sicurezza delle operazioni stesse e del titolare del mezzo di pagamento; diversamente si applica infatti quanto previsto dall'art. 12 comma 2 bis del D.lgs. 11/2010.

La definizione di autenticazione forte si rinviene nell'art. 1, lett. q bis) d.lgs. n. 11/2010 come modificato dal d. lgs. 218/2017, ove si prevede che per autenticazione forte del cliente si intende: «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 (...)».

Occorre quindi verificare dapprima se, *nel caso in specie*, l'intermediario abbia fornito elementi a sostegno dell'autenticazione e corretta registrazione e contabilizzazione delle operazioni contestate e del tipo di autenticazione predisposta; qualora infatti non fosse stata adottata dal PSP la c.d. autenticazione forte (SCA), il cliente ai sensi dell'art. 12 comma 2bis del DLGS 11/2010 risponderebbe soltanto in caso di frode, frode assente nel caso in esame. A tale riguardo, va ribadito che secondo il costante orientamento dei Collegi, il deposito dei fogli o tabulati, riproduttivi delle tracciate informatiche, corredato da apposita legenda esplicativa, deve essere ritenuto idoneo ad assolvere all'onere probatorio posto a carico dell'intermediario, nella misura in cui consenta al Collegio di verificare la corretta applicazione della S.C.A., con riferimento alle *diverse operazioni (dispositive e non)* per le quali essa è necessaria, a norma dell'art. 10 bis, d. lgs. 27 gennaio 2010, n. 11.

L'art. 10-bis, comma 1, del d.lgs. n.11/2010 dispone infatti, in conformità all'articolo 98 della PSD2 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, che *“i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi”*.

Il Collegio, in ordine alla prova della SCA, ricorda che secondo l'orientamento condiviso dai Collegi ABF, posto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali

appunto la legenda esplicativa e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione. Eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c.

Ciò premesso con riguardo al quadro normativo di riferimento come sopra delineato, ne deriva che la prova dell'autenticazione forte da fornirsi da parte dell'intermediario rappresenta, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente, in mancanza della quale il ricorso deve essere accolto.

Applicandole le regole e i principi di cui sopra al caso in esame, il Collegio preso atto che l'intermediario ha affermato che le operazioni di pagamento contestate sono state tutte correttamente autenticate con SCA mediante presentazione della carta in *modalità contactless* (circostanza questa di cui vi è idonea prova mediante i log depositati come si evince dalla dicitura "tecnologia carta" "L", sigla corrispondente a "*contact-less*"), nonché mediante corretta digitazione del PIN; con riguardo a tale secondo profilo di autenticazione e con riguardo alla asserita tokenizzazione della carta, il Collegio, preso atto che la relativa documentazione in atti non era completa sul punto, nella seduta del 16.9.2025 ha disposto una integrazione istruttoria in forza della quale invitava l'intermediario a fornire chiara evidenza dell'inserimento del PIN in relazione alle operazioni dispositive e a chiarire come fosse avvenuta la c.d. tokenizzazione (o virtualizzazione) dello strumento di pagamento, fornendo documentazione dei fattori di autenticazione a tal fine utilizzati (virtualizzazione della carta allegata dallo stesso intermediario invocata nelle controdeduzioni).

In riscontro a tale richiesta, l'intermediario ha: **a)** reso disponibile l'evidenza informatica del corretto inserimento del PIN in relazione a tutte e 3 le *operazioni dispositive*; **b)** quanto alla virtualizzazione della carta, l'intermediario non ha prodotto documentazione ulteriore ma ha riferito che, nel caso in esame, non si sarebbe verificata una vera e propria tokenizzazione della carta sui tradizionali wallet, bensì la ricorrente avrebbe subito una truffa denominata "*relay attack*", che si attua mediante l'installazione di una *app malevola nel dispositivo mobile della vittima dopo che quest'ultima ha rivelato i dati della carta e il pin al truffatore*. Il malware così installato cattura i dati della carta e le informazioni raccolte vengono poi utilizzate dai truffatori per effettuare transazioni non autorizzate.

A riprova di quanto sostenuto, l'intermediario richiama quanto dichiarato dalla stessa ricorrente nel modulo di disconoscimento del 17/03/2025, nel quale si legge che "*in data 2 marzo 2025 – giorno precedente a quello in cui sono state disposte le operazioni disconosciute – ho eseguito un pagamento on-line di euro 29,00 a favore di h-genom.com 3 Months, con il mio bancomat visa debit n. 4633456784818891. Ma non mi è mai arrivata la conferma di questo pagamento da parte del beneficiario. Il giorno successivo, dopo essermi accorta delle operazioni pos eseguite fraudolente, mi sono ritrovata con il cellulare rallentato e bloccato non potendolo più utilizzare e nemmeno spegnerlo. Come se mi fosse stata installata un'applicazione o malware o virus che non mi permetteva più l'utilizzo ed emetteva uno strano suono*".

Ciò premesso, il Collegio rileva che l'intermediario, contraddicendo quanto espressamente riferito inizialmente nelle proprie controdeduzioni, cambia versione in punto di autenticazione sostenendo che la ricorrente avrebbe subito una nuova tipologia di truffa (c.d. *relay attack*) che prescinde dalla tokenizzazione della carta, con la conseguenza che non sarebbe necessario provare la SCA rispetto a tale fase preliminare, *ma solo rispetto alle tre operazioni dispositive per le quali* – come si è visto poco sopra - l'apparato probatorio risulta invece adeguato dopo il riscontro istruttorio.

La riconducibilità della fattispecie concreta al c.d. *relay attack* (*truffa che prescinde dalla tokenizzazione della carta, con la conseguenza che rispetto a tale fase non deve essere provata la SCA da parte dell'intermediario*) è dedotta unicamente dalle dichiarazioni della ricorrente contenute nel modulo di disconoscimento sopra riportate nel virgolettato e viene allegata dall'intermediario solo in risposta alla richiesta di integrazione istruttoria di cui sopra; le dichiarazioni della ricorrente, tuttavia, non sono però adeguate a provare la conclusione avanzata dalla resistente, tenuto conto che la ricorrente non ha mai affermato di aver rivelato le proprie credenziali o i dati della carta a terzi, ma solo di aver volontariamente effettuato, il giorno prima della frode, un pagamento *online*; non constano pertanto agli atti elementi tali da far ritenere verosimile che il *malware* sia stato effettivamente installato sul dispositivo della ricorrente a causa o per effetto di tale pagamento online eseguito dalla ricorrente il giorno prima di quelli disconosciuti.

Ad avviso del Collegio, pertanto, sulla base della documentazione in atti, la versione dei fatti inizialmente fornita dall'intermediario in sede di controdeduzioni (pag. 7), versione in cui si è affermato che la carta della ricorrente era stata virtualizzata, appare maggiormente verosimile. Non essendo pertanto fornita adeguata prova della SCA con riguardo alla fase di virtualizzazione della carta con cui sono state disposte le tre operazioni disconosciute, il ricorso va accolto ai sensi dell'art. 12 comma 2 bis del Dlgs. 11/2010. Per inciso, il Collegio sottolinea che il ricorso sarebbe stato accolto anche nel caso in cui la fattispecie truffaldina in esame fosse stata ricondotta al c.d. *relay attack*; in tal caso non per mancata prova dell'autenticazione mediante SCA della fase di virtualizzazione della carta, fase che non sarebbe stata presente, bensì per *assenza di colpa grave* in capo alla Cliente: in *fenomeni analoghi* a quelli del c.d. *relay attack*, infatti, il Collegio di Coordinamento, con decisione n.3498/2012 ha escluso la sussistenza della colpa grave.

Il citato Collegio di Coordinamento ha infatti stabilito che “...Nello specifico, la ricorrente risulta essere stata vittima di un'aggressione informatica costruita attraverso un software particolarmente insidioso. A differenza che nelle fattispecie “classiche” sin qui note, dove l'aggiramento dei presidi di sicurezza e la circonvenzione del cliente ha luogo attraverso metodi ormai noti (email civetta, false comunicazioni di scadenza, invito all'aggiornamento di database e così via) che il cliente, dispiegando un minimo di diligenza, è oggettivamente in grado di schivare (anche e non secondariamente per l'accresciuta campagna di informazione che i media e gli stessi intermediari hanno da tempo ormai attuato), viceversa, nel caso in esame, la captatio ha avuto luogo attraverso un meccanismo decisamente assai più subdolo, noto da tempo – come si noterà – alla scienza informatica ma non altrettanto al pubblico dell'utenza on line, capace di sorprendere la buona fede anche di un pur normalmente attento fruitore del servizio.

La ricostruzione tecnica, che emerge in modo ineccepibile dagli atti del procedimento, evidenzia come la ricorrente sia stata indubitabilmente vittima di un software malevolo (*malware*), molto probabilmente derivato dal c.d. *malware Zeus*, che la letteratura informatica riporta siccome scoperto nel 2007, diffusosi nel 2009 e 2010, debellato dalle autorità statunitensi ma rieditato in altre consimili forme, grazie alla messa in rete dei codici sorgente (codici necessari per l'esecuzione, la manipolazione e la riprogrammazione del *malware*) disposta dalle stesse autorità.. Il principio operativo di tale meccanismo di intrusione viene definito in gergo *man in- the-browser* a significare l'interposizione che questo genere di *malware* è in grado di operare fra il sistema centrale dell'intermediario e quello del singolo utente.

Nella sua massima espressione di efficienza aggressiva, il programma malevolo, una volta annidatosi in un certo numero di computer, genera quella che in gergo suole definirsi una *botnet*, ossia per

l'appunto una rete di macchine egualmente infettate dallo stesso virus. Il malware – riconducibile alla più ampia categoria dei cc.dd. trojan ("cavalli di Troia") e dotato di sofisticate capacità di elusione dei migliori antivirus – si annida in modo silenzioso nel computer della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il malware resta completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino (targeted banks). In quel preciso istante il malware "si risveglia" ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario.... Non appare ragionevolmente ravvisabile, in siffatto contesto, alcun elemento tale da poter riqualificare siccome colposa, e tanto meno siccome gravemente colposa (ai fini di cui all'art. 12 comma 2° d. lgs. cit.), la condotta dell'utilizzatore del servizio.

Per quanto non possa negarsi che il cliente sia caduto nella tagliola ed abbia materialmente permesso l'esecuzione dell'operazione fraudolenta cooperandovi involontariamente, non è chi non veda la profonda differenza strutturale fra i dianzi citati metodi "tradizionali" di phishing e il descritto fenomeno del man-in-the-browser.

Nel primo caso, 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 che ci occupa, invece, il subdolo meccanismo di aggressione ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino, posto che l'unica "differenza" consta, come si è detto, nell'acronimo del protocollo di trasferimento, individuato come un normale "http" e non già come un "https" protetto. Ma va da sé che una simile variazione, che compare solo nella stringa di intestazione della videoschermata mischiata ad almeno cinquanta o sessanta ulteriori caratteri, barre e altri segni di punteggiatura informatica, sfugge normalmente all'attenzione di chiunque si accosti ad una pagina della rete e più che mai sfugge a chi si accosti alla pagina di un sito bancario per compiere un'operazione, dunque in un momento in cui l'attenzione dell'utente è concentrata sul contenuto della schermata e non certo sugli incomprensibili codici che la circondano e che fanno parte del normale apparato di contorno anche delle innocue consultazioni in rete."

Peraltro, nel caso in esame, ad attenuare la colpa della Cliente vi è anche la presenza dell'indicatore di anomalia di cui all'art. 8 lett. a) n. del DM 112/2007 (*tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita*), essendosi in presenza di tre pagamenti ravvicinati nello stesso giorno e quindi entro le 24 ore, pagamenti effettuati tutti con la stessa carta e presso il medesimo esercente.

Il presente ricorso, stante quanto sopra esposto, viene dunque accolto.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l’intermediario tenuto in favore della parte ricorrente alla restituzione dell’importo complessivo di euro 2.470,00 (duemilaquattrocentosettanta/00).

Dispone, inoltre, ai sensi della vigente normativa, che l’intermediario corrisponda alla Banca d’Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE