

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) RUSSO	Membro designato dalla Banca d'Italia
(PA) SCIBETTA	Membro di designazione rappresentativa degli intermediari
(PA) CLEMENTE RUIZ	Membro di designazione rappresentativa dei clienti

Relatore FEDERICO RUSSO

Seduta del 17/03/2026

FATTO

1. Parte Ricorrente, titolare di un conto presso l'Intermediario convenuto e di una carta associata a detto conto, disconosce n. 7 operazioni di pagamento eseguite mediante POS in data 03/10/2025, e segnatamente:

1. Operazione di pagamento di euro 750,00 avvenuta alle ore 21:09:32;
2. Operazione di pagamento di euro 750,00 avvenuta alle ore 21:10:12;
3. Operazione di pagamento di euro 750,00 avvenuta alle ore 21:10:32;
4. Operazione di pagamento di euro 750,00 avvenuta alle ore 21:10:54;
5. Operazione di pagamento di euro 750,00 avvenuta alle ore 21:11:12;
6. Operazione di pagamento di euro 480,00 avvenuta alle ore 21:12:19;
7. Operazione di pagamento di euro 240,00 avvenuta alle ore 21:12:46.

2. In particolare (v. denuncia 4 ottobre 2025, ore 8:36), Parte ricorrente afferma di avere ricevuto, il 3 ottobre 2025, da parte di un numero mobile non apparentemente riconducibile all'Intermediario, un SMS che la avvertiva di un presunto pagamento non autorizzato, e la invitava a contattare un numero mobile "*servizio clienti ALLERT*". Parte ricorrente contattava il numero indicato, al quale rispondeva un sedicente operatore "Ufficio Frode". Questi convinceva il Ricorrente a scaricare un'app e a inquadrare,

tramite detta app, la propria carta di credito. Poco dopo, Parte ricorrente riceveva sul telefonino notifiche di pagamenti POS sull'app, ma il sedicente operatore assicurava che sarebbero stati riaccreditati. In totale venivano eseguite, nell'arco di 3 minuti, 18 transazioni: oltre alle sette sopra indicate, altre ulteriori 11, di € 30,00 ciascuna, così per un totale complessivo di € 4.800,00.

3. Insoddisfatta dell'interlocuzione avuta a mezzo dei reclami, Parte ricorrente proponeva ricorso dinanzi a questo Arbitro Bancario Finanziario, precisando che le 11 operazioni di € 30,00 erano state, nelle more, rimborsate dall'Intermediario in data 7 ottobre 2025. Precisava, quindi, le seguenti conclusioni: *“Richiesta rimborso dell'importo di € 4470,00 non riconosciuto dall'intermediario quale importo rimborsabile”*.

4. Si costituiva l'Intermediario, precisando che la truffa in esame rientrava nello schema del c.d. “Card Relay Attack”. In particolare, il cliente era stato adescato tramite un phishing *“(nel caso in esame tramite un canale non istituzionale), quindi con un sms o con un contatto telefonico provenienti da canali non ufficiali”*, e poi indotto a installare un *malware* da un canale non ufficiale. Attraverso questo programma, i truffatori erano stati in grado di eseguire, tramite un dispositivo mobile in loro possesso, alcune operazioni tramite POS / ATM. Le operazioni, dunque, erano state autorizzate direttamente dal dispositivo del cliente (infettato dal malware), nel rispetto della SCA. L'Intermediario eccepiva, dunque, la legittimità della propria condotta e, per converso, la colpa grave del Ricorrente, precisando le seguenti conclusioni: *“Voglia l'Ill.mo Collegio adito rigettare la domanda del Ricorrente in quanto infondata in fatto e in diritto, nonché sfornita di prova, stante l'accertata legittima esecuzione delle transazioni disconosciute dal ricorrente, delle quali è stata accertata l'oggettiva regolarità e l'avvenuta corretta autenticazione e autorizzazione. In attesa di Vostre cortesie, porgiamo distinti saluti”*.

5. Parte ricorrente depositava repliche, ribadendo di avere ricevuto i vari messaggi di alert, ma che questi non erano stati utili, dal momento che le operazioni erano state compiute in un brevissimo lasso di tempo. Insisteva, pertanto, nell'accoglimento del ricorso.

6. L'Intermediario depositava controrepliche, insistendo per il rigetto.

DIRITTO

I. 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) ss.mm.ii., nonché – per quanto riguarda la *Strong Customer Authentication* (c.d. SCA) – anche delle 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).

La soprarichiamata normativa fissa una sostanziale inversione al principio dell'onere della prova fissato dall'art. 2697 c.c., chiaramente improntata al c.d. *principio di vicinanza o riferibilità della prova*, secondo cui l'onere della prova, in caso di disconoscimento di una operazione, deve essere attribuito dalla legge alla parte che a tale prova è più “vicina”, ossia al soggetto che ha predisposto la piattaforma poi utilizzata dal cliente. L'art. 10 del d.lgs. 11/2010 prevede, in particolare, che: *“1. Qualora l'utente 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”* (il comma 1 bis detta poi una regola sostanzialmente analoga in

caso di operazione disposta mediante prestatore di servizi di disposizione di ordine di pagamento). Al comma 2 la medesima norma aggiunge che: *“2 Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento(...) 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 di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente”*. Inoltre, l'art. 10-bis, comma 1, del medesimo D.Lgs. 27/1/2010 n. 11 - come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II) – statuisce che: *“Conformemente all'art 98 della Dir (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione Europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente qualora l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico...”*. La nozione di *“autenticazione forte del cliente”* è definita dallo stesso art. 1 del d.lgs. 11/2010 lett. q-bis), secondo cui si definisce tale *“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 [...]”*.

Un obbligo analogo di utilizzo di un sistema di autenticazione forte è, poi, previsto dal Reg. UE 389/2018, per tutte quelle operazioni che, a norma dell'art. 18, non possano essere considerate *“a basso livello di rischio”*.

In conclusione, in deroga ai principi generali in materia di prova, è onere dell'Intermediario dimostrare la propria diligenza (e, nell'ambito di questa, l'utilizzo di un sistema di autenticazione forte) nonché la colpa grave dell'utente.

L'inversione dell'onere della prova anzidetto, tuttavia, non può tradursi in una *presunzione assoluta* a danno dell'Intermediario né in una sorta di responsabilità oggettiva di questo: egli deve, pertanto, potere dimostrare la colpa grave del cliente e, per converso, la correttezza del proprio operato: da un lato, provando di avere adempiuto alle proprie obbligazioni con la specifica diligenza prevista (*in primis*, come detto: l'utilizzo di un sistema di autenticazione forte), dall'altro, provando l'assenza di indici di anomalia, che avrebbero potuto indurre l'operatore avveduto a bloccare l'operazione, di modo che l'operazione contestata non avrebbe potuto essere eseguita senza la colpa grave del cliente. Quanto alla prova della colpa grave, questa non può, ovviamente, essere ricavata dal semplice rispetto, da parte dell'Intermediario, delle procedure di sicurezza e dall'apparente assenza di anomalie. Tuttavia, detta prova può essere fornita anche in via presuntiva, purché si tratti di presunzioni gravi, precise e concordanti, consistenti in *“una serie di elementi di fatto particolarmente univoca e convergente, al punto che possa ragionevolmente ritenersi che l'utilizzo fraudolento sia effettivamente riconducibile sul piano causale alla condotta dell'utilizzatore”* (Collegio Coordinamento. n. 6168/2013, Collegio Coordinamento n. 22745/2019; cfr. anche Collegio Bologna, 26 luglio 2022, n. 11167 e 14 luglio 2022, n. 10560, i quali hanno ritenuto che, in caso di furto della carta di debito, il PIN fosse custodito unitamente a questa, dalla circostanza che i prelievi andarono immediatamente a buon fine, senza alcun tentativo precedente fallito).

II. Dal momento che Parte ricorrente nega di avere eseguito le operazioni, si procede all'esame della SCA.

Come correttamente ricostruito dall'Intermediario e confermato dalle risultanze documentali, la truffa è stata realizzata tramite un uso combinato del *phishing* e del c.d. *“Card Relay Attack”*. In particolare, il

cliente viene adescato tramite una tecnica di *phishing* e indotto, tramite espedienti di ingegneria sociale, a installare un *malware* da un canale non ufficiale. Il malware, a questo punto, inquadra la carta di credito recependone i dati visibili. Quindi, l'app, infettata dal *malware*, consente di veicolare il flusso di una transazione *contactless* verso un dispositivo in possesso dei truffatori, il quale dialoga a sua volta con un terminale POS o ATM. Le operazioni, dunque, vengono autorizzate direttamente dal dispositivo del cliente (infettato dal malware), che trasmette il flusso di dati al dispositivo dei truffatori e, tramite questo, all'ATM / POS.

Dai log informatici risulta, al riguardo, che il dispositivo autentico (DEVICE ID 773***C29) accedette al sistema, richiedendo il PIN, che entrò in possesso dei truffatori.

Quindi, il medesimo dispositivo – infettato dal malware – autorizzò poi le operazioni (sia pure, verosimilmente, solo in via indiretta: ossia veicolando, attraverso il *malware*, i flussi di dati da e verso il dispositivo *veicolo* in possesso dei truffatori). In pratica, i truffatori avvicinarono il dispositivo "*civetta*" al POS. A questo punto, il *malware* (installato sul dispositivo del cliente) e il dispositivo *civetta* (in mano ai truffatori) fecero da *ponte* tra il POS e l'home banking del cliente.

Dai *log*, infatti, risulta che le operazioni furono autorizzate in un canale POS tramite il dispositivo certificato del cliente (elemento di possesso, ancorché infettato dal *malware*), e la digitazione del PIN (elemento di conoscenza). Sussistono, pertanto, i requisiti richiesti per la SCA (conf. Collegio Palermo, 11791/2024).

III. Si procede all'esame della colpa grave del cliente.

In linea generale, nei casi di c.d. *spoofing*, i più recenti orientamenti dei Collegi hanno escluso la sussistenza di una colpa grave del cliente, a meno che essa non risulti da elementi ulteriori, quali, meramente a titolo di esempio, la presenza di errori nel testo del messaggio *civetta*, o, più in generale, dalla condotta del cliente nel corso della truffa.

La qualificazione come *spoofing* (nelle sue varianti), però, presuppone che i truffatori abbiano adottato una più sofisticata (ancorché di assai facile realizzazione) tecnica fraudolenta, che implica il *camuffamento* dell'indirizzo del mittente (email, sms, chiamata vocale) con un indirizzo effettivamente utilizzato dall'Intermediario *bersaglio* della truffa. Nello *spoofing*, in altri termini, il messaggio appare realmente provenire dal mittente; nel *meno insidioso phishing*, invece, i truffatori si limitano, al massimo, a modificare il campo del "*nome del mittente*", mentre l'indirizzo email (nel caso delle email) non è riconducibile all'Intermediario bersaglio della truffa. In tale seconda ipotesi va affermata la colpa grave del cliente, che viene invece oggi, come detto – dopo un contrasto protrattosi per diversi anni tra i Collegi – generalmente esclusa nei casi di *spoofing*, pur con le precisazioni sopra riportate (Collegio Palermo, 24607/2021; Collegio Palermo, 22903/2021; Collegio Milano, 12195/2022).

Nella specie, non vi è evidenza che l'SMS *civetta* provenisse da un numero apparentemente riferibile all'Intermediario. Analogamente, il numero mobile chiamato dal Ricorrente non era riferibile all'Intermediario. La fattispecie, quindi, va ricondotta nella tipologia del *phishing*, per la quale, come detto, va ravvisata la colpa grave del cliente.

A ciò si aggiunga:

- che il messaggio *phishing* "*servizio clienti ALLERT*" conteneva – almeno stando al testo trascritto nella denuncia – un errore ortografico ("*Allert*", scritto con due "l");
- che, circostanza assolutamente dirimente, il cliente scaricò e installò un software (il malware) da canali non ufficiali, ossia da un sito diverso dallo store ufficiale del produttore dello smartphone o dal gestore del S.O., compromettendo il software originale dell'Intermediario.

L'insieme di tutte le predette circostanze porta ad affermare, univocamente, la colpa grave di Parte ricorrente, che consentì il superamento di tutti i presidi di sicurezza, posti a tutela delle operazioni.

IV. La presenza della colpa grave del Ricorrente, tuttavia, non esclude la possibilità di una colpa concorrente o esclusiva dell'Intermediario almeno per alcune delle operazioni disconosciute. Invero, non può non rilevarsi il carattere *sospetto* dell'intera sequenza truffaldina, che si articolò in ben 18 pagamenti, tutti avvenuti in pochi minuti (irrilevante la circostanza che alcuni di essi siano stati poi rimborsati dall'Intermediario). A tal riguardo, il DM 30 aprile 2007, n. 112, *Regolamento di attuazione della legge 17 agosto 2005, n. 166, recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento"* all'art. 8, individua il "Rischio di frode" quando viene raggiunto uno dei seguenti parametri: "(....) b) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'articolo 7, lettera c): 1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento". Sebbene il DM 112/2007 non abbia un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, esso costituisce comunque espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'Intermediario. Tanto più che la logica ispiratrice dell'intera disciplina in materia di pagamenti elettronici è proprio di garantire il cliente, onerando l'Intermediario di adottare particolari cautele e accorgimenti tecnici per prevenire frodi. La presenza di indici di frode di cui al DM 112/2017, pertanto, pur non comportando *ex se* una automatica responsabilità esclusiva dell'Intermediario, può determinare in concreto, come nel caso concreto determina, un pur limitato concorso di colpa di questo. Secondo l'orientamento di questo Collegio, in particolare, la sussistenza del predetto indice di frode comporta il diritto del ricorrente al rimborso di una somma che può essere determinata in una misura pari al 20% dell'importo complessivamente disconosciuto (Collegio Palermo, 4148 e 4200 del 4 aprile 2024). In conclusione, va accertato il diritto della Ricorrente al rimborso della complessiva somma di € 894,00, pari al 20% delle operazioni disconosciute e non rimborsate dall'Intermediario.

V. Ogni altra domanda o eccezione assorbita.

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 894,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE