

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, tenuto della denuncia in atti, espone quanto segue:

- in data 8.5.2024, tra le 18.20 e le 18.42, riceveva alcuni sms apparentemente provenienti dall'intermediario relativi a quattro acquisti effettuati su di un noto sito internet di abbigliamento;
- riceveva quindi delle chiamate da un numero sconosciuto;
- verificato che tale numero fosse quello del servizio clienti della banca effettuava una chiamata al predetto numero ma una voce registrata la metteva in attesa;
- mentre era in attesa riceveva una chiamata proveniente sempre dal servizio clienti;
- parlava quindi con un sedicente operatore che indicava la procedura per stornare i pagamenti;

- l'operatore chiedeva di accedere all'app e di comunicare il numero utenza, di effettuare il cambio password e indicava una nuova password;
- mentre era al telefono con l'operatore, insospettita dalla situazione, si recava presso i carabinieri;
- attraverso i raggiri, i truffatori hanno eseguito un pagamento di euro 1.654,82.

Parte ricorrente, esperito infruttuosamente il reclamo, chiede all'Arbitro di condannare l'intermediario convenuto alla restituzione dell'ammontare della operazione disconosciuta pari ad euro 1654,82.

L'intermediario resistente contro deduce quanto segue:

- preliminarmente eccepisce l'assoluta indeterminatezza e genericità dell'oggetto indicato nel ricorso il quale contiene informazioni errate in quando fa riferimento "ad un pagamento con bancomat, regolato sul conto corrente, di euro 1.654,82 in favore di uno "strano" soggetto estero" ma il disconoscimento è riferito ad un bonifico;
- la ricorrente, inoltre, non fornisce prova in merito ai raggiri subiti;
- la ricorrente ha cooperato, ancorché in modo inconsapevole, alla realizzazione della truffa asseritamente perpetrata ai suoi danni sia fornendo al truffatore le proprie credenziali, come dalla stessa dichiarato, sia nelle successive fasi di autenticazione dell'operazione;
- allega i log attestanti l'autenticazione forte in tutte le fasi di autorizzazione dell'operazione;
- la mancata allegazione delle chiamate ricevute determina il rigetto del ricorso, in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e se sia pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio.

Parte resistente conclude quindi: **a) in via principale**, per il rigetto del ricorso in quanto infondato; **b) in via subordinata**, nella denegata ipotesi di accoglimento riconosca il concorso di colpa della ricorrente.

DIRITTO

Il ricorso ha ad oggetto la richiesta di rimborso di un'unica operazione disconosciuta costituita da un bonifico *on line* dell'importo di euro 1654,82 effettuato in data 8.5.2024 tramite *home banking*.

L'intermediario contesta l'indeterminatezza dell'oggetto del ricorso in quanto il ricorrente, nel compilare *il modulo di presentazione del ricorso*, fa riferimento ad un *pagamento bancomat* regolato su conto corrente; al riguardo il Collegio rileva tuttavia tale *lapsus calami* nel modulo di ricorso è superato dal *modulo di disconoscimento (allegato al ricorso)* dove l'operazione disconosciuta dell'importo di euro 1654,82 era qualificata come bonifico: in ogni caso dalla complessiva documentazione presentata dal ricorrente l'oggetto del ricorso risulta determinato.

L'orientamento dominante dei Collegi, a proposito delle operazioni che vedono il contributo causale *di cliente e frodatore*, come nel caso di transazioni inserite dal frodatore, ma eseguite, *anche solo nell'ultima fase, dal ricorrente* (ad es. tramite riconoscimento biometrico o *notifica push* come nel caso in esame), è nel senso che le stesse debbano considerarsi *non autorizzate*, e pertanto soggette al regime della PSD2 (ex multis, Collegio di Milano, decisione n. 4601/2024). Il caso in esame è caratterizzato da analoga vicenda. Osserva invero il Collegio che, nella denuncia, parte ricorrente riferisce di aver seguito le indicazioni del falso operatore e di aver collaborato al cambio password inserendo quella dettata dal truffatore e di aver poi in app accettato tutte le operazioni che lei credeva servissero invece a stornare i ("falsi ") acquisti sul sito di abbigliamento di cui aveva avuto notizia tramite sms truffaldino come riportato in fatto. Ne consegue che l'operazione di bonifico disconosciuta, pur se inserita dal truffatore, è stata autorizzata dalla ricorrente mediante l'app installata sul suo smartphone registrato. Ciò comporta che si debba procedere ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010, e cioè ad analizzare il sistema di autenticazione forte (SCA) dell'intermediario, con riferimento alle varie fasi delle operazioni contestate, che questi afferma essere state correttamente contabilizzate, registrate e autenticate. Dalla richiamata normativa e, in particolare, dall'art. 10 del d. lgs. 11/2010, discende che, qualora l'utilizzatore neghi - come nella vicenda oggetto del ricorso- di aver autorizzato l'operazione di pagamento in oggetto, gravi sull'intermediario l'onere di provare l'avvenuta autenticazione della medesima operazione, la sua corretta registrazione e contabilizzazione, nonché il mancato verificarsi di malfunzionamenti delle procedure necessarie per la sua 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 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 dell'operazione 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 Dlgs. 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 dell'operazione contestata 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.

Procedendo dunque alla verifica della SCA nei termini suddetti, dalla documentazione in atti, il Collegio rileva che l'operazione disconosciuta risulta autenticata con autenticazione forte a due fattori distinti (c.d. SCA) attraverso i seguenti passaggi:

- *sussiste una prima fase*, svolta interamente dalla cliente, di *enrollment* del proprio *device*, fase conclusasi alle ore 11.13 del 15.8.2023 alla ricorrente veniva assegnato il *New Device Id*= 8B*****9CC censito con il *serialNumber*= IR*****X.

Tale fase di *enrollment* del *device* della ricorrente era iniziata alle ore 11.09 sempre del 15.8.2023 mediante richiesta di *nuova attivazione APP* con *codice di accesso*=088*****2, *codice utente*= 08*****00 e inserimento Password. In fase di installazione dell'App sul proprio *device*, l'utente ha obbligatoriamente inserito il codice PIN di 6 cifre per accedere alla stessa App in maniera veloce senza inserire il codice utente/nickname e la password;

- indi, circa 8 mesi dopo, in data 8.5.2024 inizia la vera e propria truffa quando alle ore 18.57 viene chiesto tramite *web* dal truffatore il *reset password* relativamente al *codice di accesso* e *codice utente della ricorrente* (rispettivamente n. 088*****2 e n. 08*****00, come si è visto poco sopra): la richiesta è avvenuta dal frodatore cliccando recupera password e compilando il campo codice utente (evidentemente comunicato dalla cliente); indi il *reset password* è stato autorizzato mediante autenticazione a due fattori dalla ricorrente stessa cliccando sulla notifica *push* ricevuta sull'app token installata *sullo smartphone* della stessa ricorrente (elemento di possesso) e digitando il corretto PIN a sei cifre scelto in fase di enrollment, (elemento di conoscenza);
- la successiva fase di *accesso all'home banking* da app è avvenuta sempre in data 8.5.2024 alle ore 19:00 risultando registrato un accesso tramite App al codice di accesso e codice utente della ricorrente e dal *device registrato dalla cliente*, che dopo aver premuto su accedi, ha digitato il proprio codice PIN a sei cifre;
- poco dopo sempre in data 8.5.2024 alle 19.43 è avvenuto un ulteriore accesso all'home banking ma da sito web da parte del truffatore che ha inserito nome utente e password corretti (elemento di conoscenza) e premuto su accedi; *la ricorrente ha poi autorizzato l'accesso del frodatore dalla propria APP installata sul proprio smartphone* cliccando su "autorizzazioni in attesa - login" (elemento di possesso), ha digitato il proprio PIN a sei cifre e dopo ha premuto su "conferma" nella finestra "Autorizzi l'accesso al sito da web?" e dopo che la ricorrente ha digitato di nuovo il proprio PIN personale a sei cifre;
- l'ultima fase, quella dispositiva del bonifico, è avvenuta sempre in data 8.5.2024 verso le 19.48 da sito web della Banca (*home banking*) a cui il truffatore era acceduto come sopra; detto truffatore ha indi inserito il bonifico di euro 1654,82, bonifico autorizzato poi da app installata sul *device* della ricorrente (elemento di possesso) dove veniva digitato dalla ricorrente il PIN; in sintesi la ricorrente dalla propria APP installata sul proprio smartphone cliccando su "autorizzazioni in attesa", ha digitato il proprio PIN a sei cifre e dopo aver cliccato su "Autorizzazioni in attesa - bonifico", ha premuto su "conferma" nella finestra "Nuovo Bonifico – Autorizzi questo bonifico?" (nella videata vengono riportati tutti i dati del bonifico compreso importo e beneficiario) e dopo che la ricorrente ha digitato di nuovo il proprio PIN personale a sei

cifre l'APP ha consentito la spedizione del bonifico alle ore 19:43:54, tramite il dispositivo cellulare registrato dalla ricorrente.

La *notifica push sul device* registrato dalla ricorrente presenta il seguente testo c.d. "parlante" assimilabile ad un alert: "... *spedito pagamento... alle ore 19:43 del 08/05/2024 di 1.654,82 euro, creditore: *** SRL, iban beneficiario: IT70A *****19498*".

Alla luce di quanto sopra esposto e dalla relativa documentazione in atti, il Collegio ritiene pertanto *raggiunta la prova della autenticazione forte nel caso in esame*.

La prova dell'autenticazione forte, ai sensi della normativa sopra richiamata, non è tuttavia ancora sufficiente per esimere da responsabilità l'intermediario dovendo quest'ultimo - in aderenza al dato normativo (art. 10 del D.Lgs. 11/20105) – *fornire anche la prova della frode, del dolo o della colpa grave dell'utente*.

Il Collegio di Coordinamento, con la citata decisione n. 22745/2019, ha tuttavia ritenuto che l'intermediario possa andare esente da tale responsabilità ove indichi una serie di elementi di fatto che caratterizzano le modalità esecutive delle operazioni dalle quali possa trarsi la *prova, in via presuntiva, della colpa grave dell'utente*.

Al riguardo, l'intermediario desume la colpa grave della ricorrente, la quale ha tenuto un comportamento gravemente negligente senza il quale la presunta frode non si sarebbe mai potuta realizzare: tutta l'operatività del truffatore, infatti, sin dalla fase di accesso a quella di esecuzione del bonifico, è stata autorizzata tramite il *device identificato con il codice univoco riconducibile alla cliente*.

Parte ricorrente, a suo discarico, riferisce di aver ricevuto dei messaggi ingannatori che la informavano di acquisti eseguiti con la sua carta su un sito di abbigliamento e di aver successivamente ricevuto una chiamata dal numero verde dell'intermediario. Non ha, tuttavia, allegato né copia dell'sms civetta, né evidenza delle chiamate con le quali si è realizzata la truffa.

In casi analoghi, secondo l'orientamento condiviso dei Collegi la mancata allegazione, da parte del cliente, del messaggio civetta, determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e sia pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio (*ex multis* Collegio di Bologna, decisione n. 11920 del 26.8.2022).

Pertanto, alla luce delle circostanze del caso concreto sopra indicate, il Collegio ritiene che la realizzazione dell'operazione fraudolenta risieda nella mancata custodia delle credenziali a seguito di comportamento gravemente colposo del ricorrente (in tal senso v. Collegio di Bologna, decisioni n. 1191/2023 e n. 24745/2021; Collegio di Torino n. 13214/2021 e Collegio di Bari n. 6668/2022).

Si aggiunga che, nel caso di specie, non è integrato alcun indicatore di anomalia ai sensi del DM 2007 che possa incidere sulla valutazione, riducendola, della gravità della colpa.

Alla luce di quanto sopra esposto, il Collegio ritiene dunque che nella condotta dell'utilizzatore dello strumento di pagamento siano ravvisabili gli estremi della *colpa grave*; le conseguenze dell'operazione di pagamento disconosciuta restano pertanto esclusivamente a carico della parte ricorrente, non potendo la domanda di rimborso del relativo importo trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE