

COLLEGIO DI TORINO

composto dai signori:

(TO) BARENGHI	Presidente
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) CARATOZZOLO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) PUDDU	Membro di designazione rappresentativa dei clienti

Relatore GIUSEPPE SPENNACCHIO

Seduta del 27/04/2026

FATTO

Facendo seguito al reclamo presentato in data 16 settembre 2025 e riscontrato negativamente dall'intermediario il successivo 9 ottobre, il ricorrente si è rivolto all'Arbitro in data 12 gennaio 2026 chiedendo la restituzione della somma di €. 1.486,00=, corrispondente all'importo di operazioni disconosciute a seguito di utilizzo fraudolento dello strumento di pagamento. Ha affermato che in data 13 settembre 2025, durante la notte, degli sconosciuti hanno fatto accesso al suo conto corrente *on line* ed hanno eseguito n. 3 bonifici in favore di persone ignote, collocate in paesi esteri, per il suddetto importo complessivo.

Ha chiesto il rimborso alla banca, ma ha ottenuto risposta negativa. Ha proposto un rimborso di almeno €. 1.000,00=, ma anche questo è stato rifiutato.

Non ha mai fornito i propri codici a terzi ed ha prestato attenzione nel conservarli. Quindi la banca non ha agito con la dovuta attenzione.

Dopo l'evento, ha cominciato a ricevere *alert* in tempo reale in relazione ai prelievi.

Nelle controdeduzioni presentate in data 11 marzo 2026 l'intermediario resistente ha precisato che i bonifici sono stati eseguiti il 13 settembre 2025 da *home banking* mediante utilizzo delle credenziali del ricorrente e che già in occasione della contestazione degli addebiti ha rappresentato i motivi per i quali non ritiene di poter procedere al relativo rimborso. I ricorrenti risultano titolari di un conto corrente.

La controparte ha provveduto al formale disconoscimento dei bonifici istantanei, dichiarati fraudolenti, per un totale di €. 1.486,00=. La filiale di riferimento ha dato corso

al *recall* delle disposizioni in questione, che non ha sortito l'esito sperato, in considerazione della natura stessa dei bonifici istantanei.

Preliminarmente il ricorso va rigettato in ragione dell'assenza di una contestualizzazione puntuale degli accadimenti e della mancanza delle necessarie allegazioni documentali. Tale carenza gli impedisce di esercitare pienamente il proprio diritto di difesa, venendo meno i presupposti di trasparenza e collaborazione previsti dalla procedura.

La controparte si è limitata ad indicare, nella denuncia depositata, che in data 13 settembre 2025 ha ricevuto notifiche di pagamento sul proprio dispositivo mobile e che, dopo aver riscontrato difficoltà nell'accedere all'applicazione bancaria, ha contattato il servizio clienti, scoprendo l'esecuzione di tre bonifici istantanei. Tuttavia la ricostruzione dei fatti appare sintetica e priva di una descrizione esaustiva delle circostanze, così come di una cronologia dettagliata degli eventi necessari a corroborare le motivazioni addotte.

La mancanza di quanto sopra è anche indice della violazione del principio di cooperazione e leale collaborazione allo svolgimento della procedura. La domanda dei ricorrenti dovrebbe essere, quindi, respinta in quanto gli stessi non hanno fornito una chiara esposizione cronologica nonché un'adequata ed esaustiva allegazione dei fatti costitutivi della propria pretesa.

Pur non potendo fornire una ricostruzione dettagliata dei fatti specifici occorsi nel caso in esame, risulta tuttavia evidente che la controparte, con ogni probabilità, sia rimasta vittima di una truffa riconducibile alle tipologie di *smishing* o *vishing*. Tali forme di frode telematica si caratterizzano per la capacità di coinvolgere attivamente, seppur in buona fede, il cliente, il quale finisce per collaborare inconsapevolmente al perfezionamento dell'operazione.

La diffusione di tali fenomeni è tale che, secondo i Collegi ABF, l'adozione di una diligenza media da parte dell'utente sarebbe sufficiente a prevenire il rischio e ad evitare la consumazione della truffa. Ha da tempo avviato iniziative volte a sensibilizzare la clientela in merito alla prevenzione delle frodi informatiche.

La domanda avanzata dai ricorrenti deve essere respinta poiché non emergono elementi sufficienti a giustificare l'accoglimento. Le operazioni oggetto di contestazione sono state realizzate conformemente ai parametri di correttezza e sicurezza previsti dalla normativa vigente.

DIRITTO

L'utilizzo fraudolento è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore del d.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. Si rammenta che, secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento.

In particolare, a norma degli artt. 10 e 10-bis, d.lgs. n. 11/2010, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento contestata 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, mentre 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'art. 7. L'art. 10 prevede una precisa e graduata sequenza, in base alla quale, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo, l'antecedente logico rispetto alla prova del comportamento connotato da colpa grave dell'utente.

Pertanto *"il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima"* o *"riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo (...) fatta salva la facoltà (...) di dimostrare (...) che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento da questo prestato"* (art. 11, d.lgs. citato). D'altra parte, occorre considerare che l'utente è tenuto ad utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e deve usare l'appropriata diligenza nel conservare le chiavi di accesso ai relativi servizi (*"l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate"* recita, infatti, l'art. 7, comma 2, del citato d.lgs.).

I fatti lamentati nel ricorso denotano un episodio di utilizzo fraudolento del mezzo di pagamento senza che siano allegati elementi particolari connotanti le circostanze di fatto della frode che, secondo la denuncia allegata e quanto riportato nelle repliche, dovrebbe essere intervenuta tra la notte e la prima parte della giornata del 13 settembre 2025. Le operazioni contestate consistono in n. 3 bonifici, effettuati da *home banking*, dell'importo di €. 400,00=, €. 526,00= ed €. 560,00=, per un totale di €. 1.486,00=, eseguiti tra le ore 6:38 e le ore 14:07 del 13 settembre 2025.

Parte ricorrente, nella denuncia, ha aggiunto che i malfattori eseguivano anche n. 2 operazioni di trasferimento dal conto corrente ad una carta prepagata per complessivi €. 3.033,04=, evidentemente allo scopo di utilizzare fraudolentemente la carta per altri pagamenti. I bonifici, avvenuti in modalità istantanea, mediante utilizzo di *password* e fattore biometrico oltre ad OTP-sms, non sono stati rimborsati dall'intermediario.

Quest'ultimo ha riferito, infatti, che le operazioni contestate sono state realizzate conformemente ai parametri di correttezza e sicurezza previsti dalla normativa vigente. Del resto, sulla prova della corretta autenticazione delle operazioni contestate, l'intermediario ha prodotto le evidenze concernenti l'elenco delle operazioni sconosciute e la modalità autorizzativa, illustrate nei vari passaggi da una relazione tecnica allegata alle controdeduzioni.

Inoltre ha rilevato che, fino alla data in cui sono state disposte le operazioni sconosciute, l'utente utilizzava come strumento di sicurezza il *token* software avente seriale n. **17400 e chiave *device* **24eab. L'app era stata enrollata in data 3 luglio 2024, alle ore 15:24:23 con *nickname* **S20 su *device* di tipo android.

Risulta, per altro, una richiesta di *enrollment* della app bancaria del cliente su un nuovo *device* effettuata alle ore 2:21:23 del 13 settembre 2025. Dopo aver scaricato Y*App dallo store, l'utente ha inserito le credenziali, che sono state verificate per la *login* funzionale all'*enrollment* della nuova app di sicurezza su un nuovo *device*, con sistema operativo Apple.

Il processo di *enrollment* dell'app di sicurezza bancaria richiede l'invio di codici OTP di sicurezza ai recapiti predefiniti dal cliente, quali il numero di cellulare e l'indirizzo e-mail certificati. Infatti, al fine di autorizzare l'installazione, ha inserito l'OTP-sms di sicurezza inviato al numero di cellulare certificato e predefinito dall'utente.

L'utente ha inserito il codice OTP, che è stato validato. E' stato richiesto l'OTP vocale per completare l'*enrollment*, che è stato generato alle ore 2:23:04.

Alle ore 2:23:14 l'utente ha inserito l'OTP vocale corretto. E' stato inviato all'indirizzo e-mail predefinito e certificato dell'utente il codice OTP.

Il nuovo *token software* è stato registrato sui database della banca con chiave *device **caa, nickname G*apple 12*. Le sessioni di *login* sul dispositivo dove poco prima era stata installata la Y*App della banca, a partire da quella delle 6:32, sono state effettuate con il corretto inserimento della *password* mnemonica impostata in fase di *enrollment*. I sistemi della banca hanno valutato il corretto stato di registrazione del dispositivo ed è stata rilasciata una quantità di sicurezza applicativa random cifrata, utilizzando la chiave di cifratura del dispositivo. Il cliente ha decifrato ed ha confrontato la quantità sopra descritta con la propria chiave di cifratura, validandola.

Tutte le operazioni dispositive effettuate dall'utente sono state autorizzate secondo un protocollo di sicurezza multilivello, che prevede l'impiego di sistemi biometrici o, in alternativa, l'inserimento del PIN del dispositivo. Per ciascuna disposizione inserita dall'utente, la banca ha, inoltre, provveduto ad inviare un OTP via sms al numero di telefono collegato all'identità digitale del cliente.

Va notato che nella giurisprudenza dell'Arbitro si afferma che, a differenza delle ipotesi di furto o smarrimento dello strumento di pagamento, rispetto ai quali la mancata autorizzazione dell'operazione di pagamento sarebbe legalmente presunta, nel caso di contestazioni di utilizzi fraudolenti *on line* di strumenti di pagamento le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze. Quanto all'utilizzo dello strumento di pagamento, si è già rilevato, per altro, come nella vicenda in esame l'intermediario abbia dimostrato, mediante le schermate prodotte in atti, che le operazioni risultano autorizzate con inserimento sia delle credenziali di accesso statiche sia di quelle dinamiche, conformemente alla disciplina dei sistemi di autenticazione forte sopra richiamata.

D'altra parte occorre considerare che, secondo il consolidato indirizzo di questo Arbitro, a fronte di tale prova la domanda di parte ricorrente si rivela carente sotto il profilo delle allegazioni. Da ultimo, il blocco dello strumento di pagamento è intervenuto con notevole ritardo.

In definitiva il Collegio, tenuto conto delle richieste ed allegazioni delle parti, nonché delle condotte di entrambe, ritiene che non ricorrano ragioni per l'accoglimento del ricorso.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE