

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) SPAGNOL	Membro di designazione rappresentativa degli intermediari
(TO) BANI	Membro di designazione rappresentativa dei clienti

Relatore ANDREA BARENGHI

Seduta del 08/04/2026

FATTO

Facendo seguito al reclamo del 19 novembre 2025, riscontrato negativamente dall'intermediario il successivo 5 dicembre, la ricorrente si è rivolta all'Arbitro con ricorso del 12 dicembre 2025 per chiedere il rimborso della somma di € 29.821,69 corrispondente a n. 10 bonifici istantanei disposti tra le 21:18 del 6 novembre 2025 e le 15:17 dell'8 novembre successivo, tutti disconosciuti. Espone di aver ricevuto una mail che a causa di un aggiornamento dei sistemi richiedeva di aggiornare i dati di accesso al portale attraverso un *link* ove effettivamente inseriva le proprie credenziali. Al che il sito indicava un blocco di 48 ore, come anche l'app. Il 10 novembre 2025 non riusciva ad utilizzare l'app per accedere al sito e quindi richiedeva l'OTP sul terminale mobile scoprendo la frode. Rileva di non aver mai digitato alcun codice OTP e di non aver ricevuto nessun avviso o comunicazione circa le suddette operazioni bancarie mentre le stesse avevano luogo. Chiede quindi il rimborso della somma di € 29.821,69.

L'intermediario con le controdeduzioni presentate il 23 gennaio 2026 rileva l'accesso alla *mobile app* tramite dispositivo non in precedenza autenticato, il che richiede l'installazione dell'applicazione con registrazione e credenziali di riferimento. Dopo aver verificato le credenziali, il sistema associa l'ID utente alla sessione (previa generazione di apposito *token* di sessione restituito all'app) e verifica che al punto vendita sia effettivamente associato un conto di

pagamento attivo. La *mobile application* verifica altresì se il *device* in uso dall'utente risulta essere certificato, innescando, ove non sia così, un processo di certificazione del dispositivo, che avviene tramite inserimento in *app* di una OTP inviata via SMS al numero di cellulare della ricorrente. Le operazioni vengono eseguite mediante User ID/*password* (fattore di conoscenza) e identificativo univoco del *device* certificato associato tramite OTP alla sua utenza/notifica *push* (fattore di possesso). Proprio la ricorrente ha comunicato ai terzi le proprie credenziali di sicurezza personalizzate (segnatamente, *user-ID*, *password* e codice OTP), inserendole in una pagina accessibile tramite *e-mail*.

Chiede quindi il rigetto del ricorso.

Nelle repliche del 29 gennaio 2026 la ricorrente rileva di non aver mai comunicato né l'OTP né il PIN a terzi e che per certificare un nuovo dispositivo non viene richiesto il vecchio PIN. Rileva anche di aver ricevuto ben n. 7 codici OTP, dei quali non si capisce l'invio se la certificazione del nuovo dispositivo avveniva alle ore 17:30 e di non aver ricevuto alcuna comunicazione di *alert* circa la certificazione di un nuovo dispositivo, la connessione da un nuovo indirizzo IP e le operazioni di bonifico, e inoltre che non poteva accedere né all'*app* né al sito. In definitiva che l'intermediario non ha provato la negligenza della ricorrente in relazione alla certificazione del nuovo dispositivo, mentre appare chiaro che i sistemi informatici dell'intermediario risultano deboli, poiché il sistema di autenticazione a due fattori deve essere rispettato non solo per le operazioni dispositive, ma anche per quelle propedeutiche.

L'intermediario nelle controrepliche del 12 febbraio 2026 ulteriormente soggiunge che, con riferimento alle diverse fasi che hanno portato all'esecuzione dei bonifici contestati, ha adottato un valido sistema pluri-fattoriale basato, segnatamente, su elementi di conoscenza e possesso; che si è trattato di operazioni autorizzate dalla ricorrente, non foss'altro per l'utilizzo delle credenziali di sicurezza personalizzate, che solo la cliente poteva conoscere, e di un codice OTP che la ricorrente ha ricevuto; che per la certificazione del nuovo device non è richiesto il vecchio PIN, in quanto i fattori di autenticazione richiesti dalla normativa (username e password; OTP trasmesso via SMS) sono già presenti; che di tutte le OTP ricevute dalla ricorrente solo quella delle ore 17:27 è servita ad attivare il nuovo dispositivo (come indicato nel relativo messaggio), mentre gli altri *sms OTP* sono stati trasmessi a seguito di tentativi di accesso via *web* alla piattaforma; che la cliente non ha adottato tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate collegate al conto di pagamento; che è la ricorrente stessa ad ammettere di aver aperto un *link* pervenuto da un indirizzo *email* che non poteva in alcun modo essere riconducibile alla banca, anche alla luce dei numerosi (e palesi) indizi di anomalia contenuti nel messaggio fraudolento; che la schermata allegata alle repliche non dimostra certamente che a far data dal 06/11/2025 l'applicazione fosse inaccessibile, ma si limita a segnalare alla ricorrente che il dispositivo solitamente utilizzato "*non è più registrato*" e quindi di procedere ad una nuova certificazione; che, dopo aver aperto il *link* ricevuto via *e-mail* e inserito le proprie credenziali riservate nelle pagine web truffaldine, la ricorrente ha altresì comunicato il codice OTP, permettendo di fatto la certificazione di un nuovo dispositivo. In conclusione rileva di aver posto in essere tutti i presidi di sicurezza (e informativi) previsti dalla normativa. Insiste pertanto per il rigetto del ricorso.

DIRITTO

Le operazioni risultano effettuate senza anomalie, ciò che è puntualmente allegato e documentato dall'intermediario resistente e con corretta applicazione del sistema di autenticazione 'forte' adottato.

È stato infatti documentato da parte dell'intermediario:

- l'inserimento di *username* e *password* per l'accesso all'area personale della ricorrente da un dispositivo non certificato in precedenza alle ore 17:26:33 nella *Mobile App*;
- la rilevazione alle ore 17:26:37 che il dispositivo in uso da parte dell'utente non corrispondeva a quello associato avviando così il processo di certificazione di un nuovo dispositivo mediante generazione di un OTP inviato tramite SMS alle 17:27:44 al numero associato al profilo della ricorrente e dalla stessa fornito anche in fase di denuncia, poi in effetti utilizzato;
- alle 17:27:56 si certificava il nuovo dispositivo secondo le richieste debitamente autorizzate;
- l'utente è stato quindi ricondotto sulla pagina di *login* dell'*app*, per un ulteriore inserimento delle credenziali, che venivano effettivamente inserite alle ore 17:29:12, consentendo, previa inclusione di un PIN precedentemente creato dall'utente, di completare la SCA alle ore 17:30:52, con registrazione dell'avvenuta autenticazione a due fattori alle 17:30:53;
- previo *login* al portale *web*, alle ore 21:12:50, con l'inserimento di *username* e *password*, era poi effettuato l'accesso all'"*home banking*" attivando una nuova procedura SCA e ricevendo notifica *push* sul nuovo *device* certificato alle 21:13:49, inserendo il PIN precedentemente impostato, e completando quindi il flusso SCA alle 21:14:03.

Risulta inoltre documentato che i successivi bonifici sono stati eseguiti dall'utente, sempre previo *login* al portale *web* mediante inserimento di *username* e *password* e notifica *push* sul *device* certificato mediante l'inserimento del PIN precedentemente impostato, così completando ogni volta il flusso SCA e con ulteriore SCA utilizzando il *device* certificato/notifica *push*, come elemento di possesso, e il PIN, come elemento di conoscenza – oltre all'inserimento delle credenziali.

Si tratta di un sistema che del resto l'Arbitro ha già avuto modo di esaminare, con esito positivo (v. Coll. Bari, 17 settembre 2025, n. 8276).

Appare pertanto necessario valutare la condotta delle parti per apprezzare la colpa nella causazione dell'evento.

La ricorrente, va osservato innanzitutto, non ha compiutamente allegato le circostanze in cui la frode si sarebbe svolta, che parrebbe potersi ricondurre a un fenomeno di *phishing*. Ha dichiarato di aver fatto accesso ad un *link* ricevuto per posta elettronica, convinta della legittimità della richiesta, e di aver quindi inserito le proprie credenziali d'accesso.

Il messaggio civetta ricevuto, che la ricorrente ha debitamente allegato, contiene tuttavia incongruenze (in particolare l'uso della seconda e della terza persona singolare) cui, evidentemente, la ricorrente ha incautamente ommesso di prestare attenzione e nell'indirizzo di posta elettronica del mittente neppure compare alcun riferimento alla denominazione dell'intermediario.

La stessa ricorrente afferma di aver successivamente visualizzato un messaggio di attesa di 48 ore per un presunto aggiornamento tecnico del sito, senza tuttavia dar seguito ad alcuna verifica nei canali ufficiali dell'intermediario, mentre solo al termine di tale periodo accedeva nuovamente al portale e constatava le transazioni non autorizzate. Tuttavia va rilevato che dallo *screenshot* allegato dalla ricorrente non è possibile ricavare l'orario di ricezione degli *sms* successivi al primo (ricevuto alle ore 17:27), rispetto ai quali l'intermediario ha invece dedotto che si tratterebbe di codici per tentativi di accesso via *web*.

In proposito si deve sottolineare che, la diffusione del fenomeno di *phishing* – anche nelle varianti dello *smishing*, con l'invio di un *sms* civetta, o del *vishing* nel caso di telefonata da presunto operatore – è tale che i Collegi ABF ormai ritengono da tempo che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa (cfr., *ex multis*, Collegio di Torino, decisione n. 5143/2022).

Pertanto decisiva nel caso di specie appare la evidente mancanza di cautela della ricorrente, che ha prestato fede a un messaggio evidentemente incongruo, che la invitava a seguire istruzioni anomale, e ha inserito i propri dati riservati su un collegamento non verificato, omettendo oltretutto qualsiasi attività di verifica nell'arco delle successive 48 ore, senza allarmarsi in alcun modo nonostante l'evidente anomalia delle circostanze e anche il disagio che avevano provocato (la ricorrente ha infatti riferito che la frode si è verificata mentre stava tentando un accesso ai servizi *online*). Il Collegio ritiene che tale condotta, a fronte della compiuta dimostrazione del regolare funzionamento dei presidi di sicurezza da parte dell'intermediario, debba essere valutato in termini di colpa grave e che risulti assorbente degli altri profili di fatto del caso.

Tali elementi risultano, infatti, ad avviso del Collegio, prevalenti su quelli propri della condotta dell'intermediario, e in particolare sulla mancata documentazione dei messaggi di *alert* e sulla ricorrenza degli indici di rischio frode di cui all'art. 8 del d.m. 112/2007: quest'ultima non costituisce di per sé fattispecie di responsabilità (così anche Tribunale di Milano n. 1596/2023), ed è semmai da valutarsi con giudizio sintetico con tutti gli altri elementi del caso concreto, mentre la mancata ricezione degli *alert* relativi all'esecuzione dei bonifici, avendo l'intermediario documentato invece l'invio di un SMS contenente il codice necessario alla validazione del nuovo dispositivo, appare assorbita da quest'ultima circostanza, che dovrebbe ritenersi sufficiente (se considerata unitamente agli ulteriori SMS ricevuti e prodotti in atti da parte ricorrente a fronte di tentativi di accesso via web) per mettere sull'avviso un utente professionista, quale appunto è la ricorrente.

In definitiva il Collegio ritiene che, nella valutazione complessiva degli elementi di fatto, il ricorso non possa ritenersi fondato.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE f.f.