

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 13/03/2026

FATTO

Con ricorso del 20.10.2025, parte attrice espone che, in data 9.9.2025 riceveva un *sms* apparentemente proveniente dalla resistente, con cui veniva invitata a confermare un'operazione dispositiva ovvero a contattare un numero di telefono mobile in caso di disconoscimento; provvedeva a contattare il numero indicato nell'*sms* per disconoscere l'operazione e interloquiva con un sedicente operatore dell'intermediario, che si qualificava come addetto al servizio antifrode; questi la induceva a eseguire due bonifici, rispettivamente di € 4.900,00 e € 9.000,00, a favore di un terzo, al dichiarato fine di bloccare operazioni fraudolente a valere sul suo conto corrente; si avvedeva di essere stata vittima di una truffa e contattava telefonicamente l'intermediario per cercare di revocare i pagamenti disposti; il *contact center* riferiva che era necessario recarsi personalmente in filiale; così, il giorno successivo, si recava in filiale alle 8,30, veniva invitata a presentare denuncia querela e le veniva riferito che la

pratica di disconoscimento poteva essere avviata solo a seguito di quest'ultima; provvedeva a sporgere denuncia/querela e successivamente presentava l'istanza di rimborso alla banca, che la rigettava.

In sede di controdeduzioni, l'intermediario afferma che tutte le transazioni sono state regolarmente autorizzate e contabilizzate, senza alcuna anomalia, previa autenticazione a doppio fattore come dimostrano i *log* allegati. Sussiste la colpa grave della ricorrente, che ha seguito le indicazioni del frodatore disponendo personalmente le operazioni oggetto di ricorso. Inoltre, trattandosi di bonifici ordinari, questi potevano essere revocati entro le ore 20:00 del medesimo giorno in cui sono stati disposti, anche in autonomia dalla medesima cliente; quest'ultima non ha provveduto in tal senso e nessuna responsabilità può essere imputata alla banca, che ha tentato anche il *recall* del bonifico con esito negativo.

In sede di repliche, la ricorrente richiama l'art. 10 d.lgs. n. 11/2010 e la decisione del Collegio di coordinamento ABF n. 22745/2019, secondo cui la banca deve dimostrare non solo la corretta autenticazione delle operazioni ma anche elementi concreti idonei a provare la colpa grave dell'utente; sostiene che la frode presenti caratteristiche di particolare insidiosità, trattandosi di fenomeno di *smishing/vishing* con *sms spoofing*, in cui il messaggio fraudolento appare formalmente proveniente dal canale ufficiale della banca ed è inserito nello stesso flusso comunicativo dei messaggi autentici; richiama l'orientamento ABF secondo cui, in tali ipotesi, la particolare sofisticazione della truffa attenua o esclude la colpa grave dell'utente e cita a conferma le decisioni del Collegio di Milano n. 7564/2025, del Collegio di Bologna n. 7036/2025 e del Collegio di coordinamento n. 6790/2025. Deduce, inoltre, profili di responsabilità dell'intermediario nella gestione dell'allarme successivo alle operazioni, evidenziando che la cliente aveva tentato immediatamente di revocare i bonifici e aveva contattato il numero verde della banca la sera stessa, senza ottenere interventi utili, mentre la segnalazione al presidio antifrode sarebbe stata inoltrata solo il giorno successivo: richiama sul punto pronunce ABF (tra cui Collegio di Milano n. 6790/2025 e Collegio di Bari n. 7228/2025) che qualificano ritardi analoghi come criticità organizzative dell'intermediario idonee a fondare quantomeno un concorso di responsabilità.

In sede di controrepliche, l'intermediario contesta la qualificazione della frode come sofisticata, evidenziando che il numero mittente dell'*sms* (344***1) e il numero telefonico utilizzato nei contatti (350***86) non appartengono alla banca e che il messaggio non risulta inserito tra quelli genuini ricevuti dall'intermediario. Sostiene inoltre che il messaggio presentava evidenti errori grammaticali e sintattici che avrebbero dovuto essere riconosciuti dall'utente medio con l'ordinaria diligenza. Rileva che la ricorrente non avrebbe fornito prova della riconducibilità dei contatti telefonici alla banca né prodotto *screenshot* di messaggi istituzionali con cui confrontare l'*sms* ricevuto. Ritiene pertanto inconferenti i precedenti ABF richiamati dalla ricorrente, sostenendo che tali decisioni riguardano ipotesi di *sms* apparentemente riconducibili ai canali ufficiali della banca, circostanza che nel caso di specie esclude. Aggiunge che la cliente avrebbe potuto evitare la frode, essendo consapevole del *cut-off* dei bonifici alle ore 20 e avendo ricevuto alle ore 19:21 un *sms* di conferma relativo a bonifico verso nuovo beneficiario, con importo peraltro diverso da quello indicato nel messaggio fraudolento. Conclude chiedendo il rigetto del ricorso per infondatezza.

In relazione alle rispettive argomentazioni, la ricorrente chiede all'Arbitro il rimborso dell'importo complessivo di € 13.900,00. Dal canto suo, l'intermediario chiede al Collegio di respingere il ricorso.

DIRITTO

La controversia ha ad oggetto due operazioni di bonifico ordinario, materialmente eseguite dalla ricorrente, a ciò indotta dai frodatori. L'intermediario afferma in particolare che l'operazione è stata autenticata mediante OTP generata in maniera silente. La funzionalità *Mobile Token*, disponibile nell'*app* dell'intermediario, consente di generare *password* dispositive per confermare le operazioni

previste dal servizio di *internet banking* (bonifici, ricariche, etc.) e i pagamenti effettuati con carta di credito su siti di *e-commerce*; l'intermediario sottolinea che il suo funzionamento si basa su un sistema multi fattoriale. Una volta attivato il *Mobile Token*, l'operazione è disposta mediante l'inserimento del codice OTP dallo stesso generato (fattore di possesso), previo inserimento del c.d. MPIN (fattore di conoscenza). La componente del "possesso" è integrata in presenza di una OTP generata da un *device* (in questo caso, da un *software token generator*). L'intermediario allega i relativi *log*, da cui si conferma che le operazioni di pagamento risultano correttamente autenticate, registrate e contabilizzate e che non è emerso alcun malfunzionamento o compromissione dei sistemi. Il Collegio ritiene *compliant* alla SCA la modalità autorizzativa che fa leva sull'inserimento di credenziali statiche (es. PIN) e del codice OTP generato da un *mobile token (token app)*: cfr. Collegio di Roma, decisione n. 6634/2021.

Dalla ricostruzione dei fatti per cui è ricorso, la ricorrente è rimasta vittima di una frode riconducibile al c.d. *smishing*. Essa dichiara di aver ricevuto un *sms* in data 9.9.2025 recante la denominazione dell'intermediario, contenente l'invito a contattare un numero di telefono in caso di disconoscimento di un'operazione dispositiva. Avrebbe poi chiamato il numero di telefono mobile ivi indicato, interloquendo con un sedicente operatore dell'intermediario che l'avrebbe indotta a disporre le operazioni oggetto di ricorso. Produce evidenza dell'*sms* ricevuto, ma non del registro chiamate. Dal messaggio emerge che esso non si inserisce in coda ad altri *sms*; il mittente della *chat* non reca il nominativo dell'intermediario; il numero di cellulare che si invita a chiamare non è riconducibile all'intermediario; sono presenti errori grammaticali e/o sintattici ("se non è stata lei *chiama* al..."). Dopo aver contattato il numero di cellulare indicato nell'*sms*, la ricorrente dichiara di aver richiesto telefonicamente alla banca di disporre la revoca dei bonifici. Produce evidenza della chiamata effettuata al servizio clienti dell'intermediario, a partire dalle ore 21:00 del giorno della frode. Sul punto, l'intermediario ha specificamente contestato che la chiamata fosse tardiva, in quanto la revoca dei bonifici poteva essere disposta entro le ore 20:00. Inoltre, la ricorrente avrebbe avuto il tempo di richiedere la revoca in quanto la prima operazione dispositiva è stata oggetto di *sms alert* ricevuto alle 19:21. Siffatta circostanza assume un evidente rilievo per contrastare la contestazione, avanzata dalla ricorrente, di negligenza dell'intermediario nella gestione della richiesta di revoca dell'operazione.

L'orientamento unanime dei Collegi territoriali ritiene che, quando l'operazione è eseguita per intero dal pagatore, deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2. I Collegi convengono che, in questi casi, non è configurabile una responsabilità oggettiva del PSP. Il Collegio potrà comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode. Nel caso di specie, però, anche alla luce del rilievo che la linea telefonica utilizzata per il messaggio civetta e per interloquire poi con il truffatore non sono riconducibile all'intermediario, non vi sono gli estremi per configurare un concorso di responsabilità della banca.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE