

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) NASO	Membro di designazione rappresentativa dei clienti

Relatore STEFANO DEPLANO

Seduta del 04/12/2025

FATTO

Parte ricorrente rappresenta che: i.) in data 28 gennaio 2025 ha ricevuto tre SMS apparentemente provenienti dalla Banca convenuta che la informavano di tre bonifici in uscita dal conto; ii.) poco dopo è stata contattata da un'utenza telefonica, parimenti riconducibile alla resistente; iii.) durante la chiamata l'interlocutore le ha riferito che stava cercando di stornare le predette operazioni e, a tal fine, la invitava ad accettare un'autorizzazione che le era stata inviata sul telefono; iv.) dato seguito alle indicazioni e avendo notato il saldo diminuire si è insospettita e ha preso contatto con il servizio clienti della Banca, avvedendosi dell'esecuzione di un bonifico fraudolento di importo pari a 1.900,00 (millenovecento/zero) euro.

Parte resistente riferisce che: i.) l'operazione disconosciuta risulta essere stata eseguita con la collaborazione attiva della cliente e senza anomalie o malfunzionamenti; ii.) il bonifico risulta autorizzato tramite autenticazione forte; iii.) non risultano versati in atti gli SMS truffaldini; iv.) la chiamata fraudolenta non ha natura sofisticata ma rientra nella "comune" ipotesi del *vishing*; v.) la ricorrente ha negligenemente dato seguito ad indicazioni telefoniche fornite da persona sconosciuta; vi.) la cliente non ha utilizzato l'APP di verifica del numero chiamante implementata dalla Banca al fine di prevenire le frodi; vii.) risulta evidente la colpa grave della cliente la quale ha dato credito al truffatore senza avvalersi dei sistemi di protezione approntati dall'Intermediario.

Non risultano presentate né repliche né controrepliche.

Parte ricorrente disconosce un bonifico di importo pari a 1.900,00 euro e ne chiede il rimborso.

Parte resistente insiste per il rigetto del ricorso.

DIRITTO

1. – La controversia ha ad oggetto il disconoscimento di un bonifico istantaneo *on line*, effettuato in data 28 gennaio 2025, di importo pari a 1.900,00 euro.

2. – In via preliminare occorre esaminare l'eccezione sollevata dall'Intermediario in merito alla normativa applicabile. Parte resistente, in dettaglio, deduce che l'operazione disconosciuta non possa considerarsi non autorizzata poiché effettuata "sotto dettatura" da parte della stessa ricorrente.

2.1. – Dalla denuncia versata in atti, invero, emerge che la ricorrente si è soltanto limitata a validare la notifica *push* ricevuta in APP per autorizzare il bonifico. Nel ricorso introduttivo alla controversia, del pari, dapprima è dichiarato che «l'operazione di bonifico [è stata] disposta da un truffatore» e, successivamente, si precisa che le «richieste di bonifico non [sono state] inserite dalla sottoscritta ma disposte con frode». Dai *log* prodotti da parte resistente, infine, si evince che l'accesso è avvenuto dalla pagina *web* dell'area riservata dalla quale è poi partita la notifica *push* transitata sul *device* della ricorrente la quale l'ha autorizzata su indicazione del truffatore.

2.2. – Tanto posto, l'eccezione in esame non merita di essere accolta.

3. – L'operazione contestata è stata effettuata sotto la vigenza del d.lgs. n. 11 del 2010, così come modificato dal d.lgs. n. 218 del 2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). In base a tali disposizioni, come applicate da questo Arbitro (cfr. Coll. Coord., dec. n. 22745 del 2019), occorre volgere l'attenzione a due dirimenti profili disciplinari. In primo luogo, è l'Intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza che le operazioni sconosciute siano state autenticate con un c.d. "Sistema di autenticazione forte" (SCA), posto che ai sensi del comma 2 *bis*, art. 12, d.lgs. n. 11 del 2010, come inserito dal d.lgs. n. 218 del 2017 «salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente». In secondo luogo, è sempre l'Intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.

4. – Con riferimento al primo profilo, visti i *log* versati in atti, parte resistente dimostra che tanto l'accesso all'APP tanto l'autorizzazione del bonifico sono avvenuti tramite un'autenticazione a doppio fattore. Nel dettaglio, la cliente ha autorizzato l'operazione digitando il codice segreto (fattore di conoscenza) ed ha autorizzato la notifica *push* sul proprio *smartphone* (fattore di possesso). Tale sistema è già stato ritenuto SCA *compliant* da parte di codesto Collegio (cfr. Coll. Roma, dec. n. 3343 del 2025).

4.1. – L'Intermediario ha quindi dato prova di essersi dotato di un sistema di autenticazione forte in linea con la normativa di settore.

5. – Con riferimento al secondo profilo innanzi richiamato, parte ricorrente ha ricevuto alcuni SMS apparentemente provenienti dall'Intermediario, i quali segnalavano la richiesta di un bonifico non autorizzato e preannunciavano la chiamata da parte di un operatore. I messaggi appaiono genuini: sono privi di errori grammaticali e/o sintattici, indicano come mittente il nominativo della Banca e sono seguiti da una comunicazione effettivamente proveniente dall'Intermediario.

6. – La ricorrente ha quindi ricevuto la chiamata preannunciata dal messaggio truffaldino. Sulla base dello *screenshot* della lista-chiamate versato in atti è possibile ritenere che il numero chiamante collimi con un numero di assistenza dell'Intermediario per le chiamate provenienti da cellulare e dall'estero. Tanto consente di reputare che il raggio cui è causalmente riconducibile l'operazione sconosciuta si articoli – oltre che in un SMS *spoofing* – anche in un *caller ID spoofing* ossia un'ipotesi di frode da reputarsi ben più insidiosa rispetto al "classico" *vishing* (Coll. Roma, dec. n. 8749 del 2024; Coll. Milano, dec. n. 22105 del 2021).

7. – Attesa la particolare insidiosità della macchinazione posta in essere dai truffatori (composta dell'invio di SMS decettivi che anticipano una chiamata apparentemente proveniente dal numero dell'Intermediario) la condotta della correntista che ha autorizzato il pagamento reputandolo imposto dalla necessità di stornare operazioni non autorizzate appare, in questo caso, esente da colpa grave.

8. – In senso opposto, tuttavia, la Banca deduce che la ricorrente avrebbe omesso di utilizzare l'APP di verifica del numero chiamante implementata proprio al fine di prevenire le frodi. Secondo parte resistente tale accortezza avrebbe permesso, da una parte, di stabilire con certezza che la chiamata non proveniva da un operatore dell'Intermediario e, dall'altra parte, di sventare la frode in corso. Tale

omissione, sulla base dell'eccezione prospettata, integrerebbe gli estremi di un comportamento gravemente colposo da parte della ricorrente.

9. – Il rilievo non appare condivisibile.

10. – La direttiva PSD2 detta per gli Intermediari un regime di responsabilità svincolato dal modello di imputazione fondato sulla colpa, oltre che caratterizzato da un evidente *favor* a vantaggio degli utilizzatori (in piena coerenza, del resto, con lo spirito *customer friendly* dell'intera normativa). Si vuole dire che il PSP è in ogni caso responsabile per l'operazione abusiva salvo che dimostri che quest'ultima sia stata resa possibile dalla condotta fraudolenta o gravemente colposa dell'utilizzatore.

11. – Il legislatore pone in capo al cliente alcuni obblighi tesi a prevenire l'utilizzo indebito degli strumenti di pagamento (art. 7, d.lgs. n. 11 cit.). Il titolare della carta è infatti tenuto a «utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso [...]», a «comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza» e, da ultimo, a proteggere le credenziali di sicurezza personalizzate.

11.1. – Il disposto normativo non prevede, invece, un obbligo di adoperare in ogni caso gli ulteriori strumenti di sicurezza predisposti dall'Intermediario per scongiurare la realizzazione di una frode nell'utilizzo dei sistemi di pagamento. A tali misure, tuttavia, deve essere riconosciuto un ruolo dirimente quando le modalità con cui è realizzata la frode avrebbero dovuto allertare un utente mediamente avveduto.

11.2. – In caso di SMS decettivo caratterizzato da evidenti errori di tipo grammaticale o sintattico, ad esempio, appare senz'altro ragionevole gravare il cliente dell'onere di attivare il sistema predisposto dall'Intermediario al fine di assicurarsi della genuinità della conversazione e dell'identità dell'interlocutore. In difetto di tale accortezza risulterebbe non soltanto provata la colpa grave dell'utilizzatore ma anche escluso il concorso di colpa da parte del prestatore del servizio di pagamento al quale non si potrebbe certo contestare di non aver approntato i mezzi tecnici utili a garantire un sistema di pagamento efficace e sicuro (cfr., in termini, Coll. Roma, dec. n. 9491 del 2025).

13. – Se invece, come accade nell'ipotesi oggetto di scrutinio, le circostanze di fatto depongono nel senso di non lasciar dubitare della riferibilità all'Intermediario delle comunicazioni pervenute, allora non appare congruo obbligare il cliente – contro il dettato di legge e la complessiva *ratio* della direttiva richiamata – ad effettuare un controllo tramite i sistemi di sicurezza predisposti dal PSP prima di dare esecuzione all'operazione.

14. – Stabilito che risulta provata la SCA in relazione all'operazione controversa ma escluso che la condotta della ricorrente possa reputarsi gravemente colposa, in definitiva, il ricorso appare fondato e meritevole di integrale accoglimento.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 1.900,00.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE