

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) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 06/02/2026

FATTO

La parte ricorrente espone quanto segue:

- è cliente dell'intermediario resistente;
- il 28/01/2025 alle ore 15:48, riceveva sul proprio telefono cellulare un SMS con mittente l'intermediario che si collocava in coda agli altri sms già più volte pervenuti dallo stesso mittente. Il messaggio così recitava: "Accesso eseguito da un nuovo dispositivo Apple iphone 14 Pro, se disconosci chiama il nostro servizio assistenza al n. +393508281828";
- il messaggio era scritto in italiano corretto, senza errori grammaticali, non riportava altre indicazioni né link su cui cliccare; quindi, vedendo che proveniva dal proprio intermediario pensava che si trattasse di una comunicazione ufficiale e, allarmato dal messaggio ricevuto, chiamava il numero indicato al quale rispondeva una persona senza inflessioni dialettali, che si qualificava come operatore dell'Ufficio Antifrode della banca, indicando anche il proprio nome e numero di matricola;
- perveniva immediatamente un sms che informava il ricorrente di essere in contatto con un presunto operatore che lo informava che risultava una disposizione di bonifico di € 1.550,00 dal proprio conto corrente e che, per annullarla, era necessario simulare un "contro bonifico" del medesimo importo, indicandogli anche l'iban sul quale disporre l'accredito e il beneficiario;

- nel frattempo, pervenivano altri sms che confermavano le parole dell'interlocutore. Perveniva anche un SMS che riportava la dicitura "Modalità simulazione in corso" e un altro con la dicitura "Pagamento bloccato correttamente, il saldo sarà ripristinato al termine dell'operazione.";
- credendo di aver bloccato un bonifico fraudolento, in realtà lo aveva disposto senza rendersene conto, seguendo le istruzioni dell'interlocutore che reputava essere un incaricato dell'Ufficio Antifrode della propria banca;
- queste operazioni si ripetevano per altre 2 volte, con un bonifico di € 1.542,00 e un altro di € 910,00 per un totale di € 4.002,00 oltre € 5,43 di commissioni;
- la conversazione telefonica si prolungava per diverse ore arrestandosi più volte e riprendendo successivamente, dalle ore 15:49 alle ore 20:19;
- perveniva un ultimo SMS delle ore 20:04 con cui il ricorrente veniva informato che la sua pratica era in fase di elaborazione e che il saldo del conto era "supervisionato" dal dipartimento di sicurezza;
- certo di aver sventato, con l'aiuto dell'intermediario, un tentativo di frode a suo danno, seguiva le ultime istruzioni dell'interlocutore che lo induceva a disinstallare l'App confermando, anche via sms, un appuntamento telefonico ulteriore per il giorno seguente alle ore 12:30;
- il giorno successivo, non ricevendo alcuna chiamata all'orario concordato, si insospettiva e verificava che i 3 bonifici risultavano in addebito;
- si recava quindi allo sportello della propria filiale dove gli veniva confermato di essere stato truffato ma nessun dipendente della banca, in quella circostanza, lo informava della necessità di sporgere denuncia e della possibilità di presentare il modulo di disconoscimento e reclamo;
- il 04/03/2025 si recava quindi presso un'associazione consumatori da cui veniva avvisato della necessità di presentare denuncia e di recarsi in banca con la denuncia presentata per procedere alla contestazione delle operazioni;
- il 05/03/2025, presentava denuncia e provvedeva alla compilazione del "Modulo contestazione importi" in filiale;
- il comportamento tenuto dalla filiale di riferimento va stigmatizzato in quanto contrario alla diligenza professionale richiesta anche in considerazione del fatto che non ha permesso al ricorrente di potersi tempestivamente tutelare;
- giungeva una pec in risposta al reclamo che informava "le strutture preposte che hanno eseguito le verifiche confermano che accesso e disposizioni siano avvenute con corretto riconoscimento delle credenziali e delle password dispositive" non menzionando il fatto che la richiesta di rimborso del denaro fraudolentemente sottratto non era stata accolta;
- l'art. 10 del dlgs. 11/2010 dispone che l'onere di provare la frode, il dolo o la colpa grave dell'utente è posto dalla normativa a carico dell'intermediario (art. 10 comma 2) ma questi nella propria risposta negativa, non fornisce alcuna prova al riguardo;
- dagli sms pervenuti ed allegati al ricorso, si può notare che: i) sono tutti pervenuti incasellandosi cronologicamente uno di seguito all'altro sotto il medesimo mittente; ii) non contengono link e dunque il ricorrente non ha cliccato nulla né ha quindi inserito le proprie credenziali su siti clone; iii) sono scritti in italiano corretto, senza errori grammaticali o di sintassi tali da poter ingenerare nel ricorrente il sospetto che potesse trattarsi di una frode;
- è dunque caduto vittima di spoofing e vishing, modalità di truffa ritenute particolarmente insidiose dalla giurisprudenza di codesto arbitro, senza che possa addebitarsi allo stesso alcuna colpa grave, unico motivo che potrebbe essere posto alla base di un rifiuto al rimborso delle operazioni disconosciute mentre l'intermediario non fornisce alcuna prova di una eventuale colpa grave;
- la decisione n. 22745/2019 del Collegio di Coordinamento ha enunciato il seguente principio di diritto: "la previsione di cui all'art. 10, comma 2, del d.lgs. n. 11/2010 in ordine all'onere posto a carico del prestatore del servizio di pagamento della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere

probatorio, essendo necessario che l'intermediario provveda specificatamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione da cui possa trarsi la prova, in via presuntiva della colpa grave dell'utente.”;

- la suddetta decisione rileva inoltre come “il Collegio di coordinamento, in più occasioni, abbia precisato che la disciplina in esame istituisce “un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art.7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento” (Coll. Coord., decisione n. 3947 del 24.6.2014. In senso conforme: Coll. Coord. Decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014);

- non può essergli addebitato un comportamento fraudolento né una colpa grave, avendo posto fiducia nei messaggi pervenuti che risultavano provenire dalla propria banca e alla telefonata, nella quale il truffatore ha mostrato di essere già a conoscenza di tutti i suoi dati identificativi; le parole del truffatore venivano di volta in volta confermate dagli sms che precedevano e seguivano quelli ufficiali della banca di notifica delle operazioni disposte;

- richiama la decisione del Collegio di Roma n. 1309 del 10/02/2023, che così recita: “Nell'ambito della classica distinzione tra metodi tradizionali di frode e subdoli meccanismi di aggressione, il Collegio di Roma – richiamando un punto della motivazione della pronuncia del Collegio di Coordinamento n. 22745/2019 – ha ricondotto alla categoria delle frodi sofisticate le intrusioni truffaldine tramite “sms spoofed”. Si tratta di ipotesi di smishing in cui il messaggio reca, quale mittente, la denominazione dell'intermediario, in modo tale che il testo si inserisca, nei moderni smartphone, all'interno della conversazione contenente messaggi genuini (effettivamente provenienti dall'intermediario). Nei casi di spoofing i Collegi territoriali ABF hanno in generale evidenziato l'insidiosità del meccanismo di aggressione, consistente nell'invio dell'sms dall'utenza dell'intermediario, tale da rivelare criticità organizzative del servizio di pagamento offerto. Tuttavia hanno parimenti osservato che talvolta il testo del messaggio civetta presenta indici di evidente inattendibilità (quali ad esempio errori grammaticali o sintattici) o di anomalia (quali ad esempio l'invito a selezionare un link in nessun modo riferibile all'intermediario) che dovrebbero far allertare l'utente avveduto. Si ritiene quindi che nelle fattispecie di spoofing non sia generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione, a meno che non si rinvenivano i suddetti indici di inattendibilità o anomalia del messaggio.” (...omissis...) “In riferimento al messaggio truffaldino inviato alla ricorrente si osserva che (i) il mittente reca la denominazione dell'intermediario; (ii) al messaggio truffaldino sono accodati i messaggi genuini inviati nell'ambito del processo di autenticazione dell'operazione contestata; (iii) il messaggio non sembrerebbe presentare degli errori grammaticali”;

- la decisione richiamata viene confermata dalla recente decisione n. 3727/24 del 25/03/2024, che così recita: “ Quanto al messaggio ricevuto da parte ricorrente, alla luce della documentazione in atti risulta che l'SMS “civetta” si è inserito nella sequenza dei messaggi genuini provenienti

dall'intermediario e non presenta errori grammaticali; il contatto del mittente risulta corrispondente a quello dell'intermediario(omissis)... Secondo l'orientamento consolidato finora adottato dai Collegi, quando il cliente è vittima di questo tipo di truffa non può essere in genere ravvisata una sua colpa grave, salvo che il messaggio civetta presenti indici di evidente inattendibilità o anomalia che dovrebbero allertare l'utente avveduto; in quest'ultimo caso può essere riconosciuto un concorso di colpa per l'utente a causa della sua grave negligenza che agevola la truffa. Allo stato, nonostante la maggiore diffusione di campagne informative sul tema, lo spoofing conserva ancora il carattere di insidiosità (cfr. Collegio di Roma, decisione n. 1625/2022)"

- secondo la giurisprudenza ABF, nel caso in cui il "messaggio civetta" non presenti indici di anomalia o inattendibilità non può ravvisarsi la colpa grave del cliente, data l'insidiosità del meccanismo di aggressione: si considera indice di evidente inattendibilità la presenza di errori grammaticali nel testo del messaggio ricevuto, condizione che non si è presentata nel caso in esame nel presente ricorso, non può pertanto configurarsi una sua negligenza grave che abbia agevolato la truffa subita; pertanto, chiede l'accoglimento del ricorso e il rimborso di complessivi € 4.007,43, oltre interessi legali dalla data delle operazioni fraudolente fino alla data dell'effettivo rimborso da parte dell'intermediario.

Nelle controdeduzioni, l'intermediario eccepisce quanto segue:

- il ricorrente, titolare del conto corrente n. ****6758, dichiara di aver ricevuto il 28/01/2025 alle ore 15:48 sul proprio telefono cellulare un SMS che si collocava in coda agli altri sms già più volte pervenuti dallo stesso mittente che lo informava di un accesso eseguito da un nuovo dispositivo telefonico e lo invitava a chiamare il servizio assistenza ad un numero di cellulare se disconosceva l'accesso;
- allarmato dal messaggio ricevuto, chiamava il numero indicato al quale rispondeva una persona che si qualificava come operatore dell'Ufficio Antifrode della banca e lo induceva a fare 3 bonifici con beneficiario sconosciuto;
- i bonifici disposti il 27.6.2025 alle ore 18.54 e 19:04 a seguito della truffa sono: i) stati eseguiti tramite l'App della banca installata sul telefono di parte ricorrente; ii) andati a buon fine al primo tentativo poiché l'autorizzazione degli stessi è stata concessa dalla cliente che li ha concretamente disposti inserendo manualmente l'importo, il nominativo del beneficiario, un nominativo a lui sconosciuto e inserendo manualmente, in fase di esecuzione, l'iban del beneficiario indicato dai truffatori;
- la truffa si è potuta realizzare solo attraverso il contributo di parte ricorrente, che non si è limitata solo a fornire i codici di accesso all'APP Mobile del suo device ma ha pure disposto dalla propria App i bonifici per un totale di € 3.340,00 disponendo quindi il trasferimento dei fondi dal proprio c/c al beneficiario sconosciuto e autenticando l'operazione con utilizzo di credenziali e autorizzazioni del bonifico con password 3DS generata da device associato all'utenza di cellulare collegata alla cliente stessa;
- senza il contributo di parte ricorrente stessa la truffa non avrebbe mai avuto luogo e la "colpevole credulità" della cliente, che riteneva di dialogare con un operatore della sua banca, ha permesso il compiersi della truffa ai suoi danni;
- i dati di contatto possono essere recuperati dai truffatori in svariati modi: è sufficiente violare le difese di qualsiasi infrastruttura collegata a società di servizi che ottengono accrediti tramite SDD o RID per reperire elenchi di nominativi con numeri di telefono associati ed IBAN; un truffatore può eseguire la frode subita dalla cliente semplicemente conoscendo questi tre dati: non ha bisogno di violare la sicurezza della Banca anche perché, se ne fosse davvero in grado, probabilmente non vi sarebbe nemmeno ragione di dover contattare il cliente;
- sul caso, non c'è alcuna responsabilità adducibile alla banca che può valutare l'intenzione di eseguire un pagamento da parte di un cliente solo sulla base dell'utilizzo corretto dei codici per autorizzare una transazione (nel rispetto delle normative vigenti) e non sulla base delle motivazioni che lo spingano a farlo;
- rileva la decisione 18346/21 del Collegio di Palermo che ha così statuito: "Non sussiste la responsabilità dell'intermediario neanche con riguardo al comportamento tenuto successivamente

all'effettuazione del bonifico. Il d. lgs n. 11/2010 prevede all'art. 17 l'irrevocabilità degli ordini di pagamento. Dispone inoltre al quarto comma che nel caso di cui all'articolo 15, comma 2, vale a dire quando "l'utente e il prestatore di servizi di pagamento di cui egli si avvale concordano che l'esecuzione dell'ordine di pagamento sia avviata in un giorno determinato o alla fine di un determinato periodo o il giorno in cui il pagatore ha messo i fondi a disposizione del prestatore di servizi di pagamento", "l'utente può revocare un ordine di pagamento non oltre la fine della giornata operativa precedente il giorno concordato".

- la ricorrente procedeva ad inoltrare reclamo il 24 aprile 2025 per richiedere il rimborso che riceveva risposta negativa il 7 luglio 2025 in quanto dalle verifiche effettuate, non risultava alcuna intrusione nei sistemi informatici della banca;
- in presenza di coordinate IBAN dei beneficiari corrette, l'accredito viene eseguito automaticamente, posta la perfetta corrispondenza tra beneficiario indicato ed effettivo intestatario;
- allo scopo di prevenire eventi fraudolenti anche simili a quello in esame, ha da tempo pubblicato, sul proprio sito web, informazioni relative ai rischi e ai suggerimenti utili ad evitare le frodi; non può rispondere dell'operatività online dei singoli clienti, ma dispone presidi generali di sicurezza, e sensibilizza i propri Clienti, attraverso i principali canali di comunicazione, perché prestino attenzione a segnali di possibili tentativi di frode;
- richiama la decisione N. 9934 del 10 aprile 2019 dove si rileva che:[...la valutazione dell'adeguatezza sia del sistema di protezione delle transazioni online adottato all'intermediario sia della sua organizzazione, funzionale alla segnalazione ed al blocco di eventuali operazioni anomale, quali espressioni della diligenza professionale dallo stesso esigibile ai sensi dell'art. 1176, comma 2, c.c.; per altro versante, l'osservanza, da parte dell'utilizzatore dei servizi di pagamento, delle disposizioni previste dagli artt. 7 e 9, d.lgs. 11/2010. È noto che tale disciplina mira a salvaguardare l'utente dei servizi di pagamento, come attestano: 1) la c.d. inversione dell'onere della prova in tema di responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento (art. 12, d.lgs. 11/2010, nel testo modificato dal d.lgs. 218/2017); 2) il dovere del prestatore del servizio di pagamento di "assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7" (art. 8, d.lgs. 11/2010, nel testo modificato dal d.lgs. 218/2017). In particolare, l'utilizzatore è tenuto alla rigorosa osservanza di una serie di obblighi, che vanno dalla custodia delle credenziali di autenticazione, all'adozione, secondo diligenza, delle normali cautele che è ragionevole attendersi nell'uso dello strumento di pagamento (art. 7, d.lgs. 11/2010, nel testo modificato dal d.lgs. 218/2017)].
- rinvia al Regolamento Delegato UE 2018/389 - che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri - in merito alla sicurezza delle operazioni on line - specificando a tal riguardo che la banca aderisce pienamente a tali norme;
- l'intenzione della cliente era quella di eseguire i bonifici per un totale di € 3.340,00 in favore di un beneficiario sconosciuto, seguendo pedissequamente le indicazioni dell'asserito operatore della banca, senza mai insospettirsi e porsi il minimo dubbio in corso d'opera sulla correttezza della disposizione che stava eseguendo;
- parte ricorrente non comunicava anomalie sul telefono o sulla sim e che pertanto non possono essere contestate intrusioni informatiche né vulnerabilità del sistema, né peraltro viene fornita documentazione a supporto;
- è confermato che i bonifici sono stati compiuti "con il contributo causale decisivo alla perpetrazione della frode dalla Ricorrente, la quale deve aver eseguito tutte le indicazioni ricevute dal malfattore rilevatisi sufficienti al compimento" dello stesso (cfr decisioni 9263/22, 9242/22 e 9254/22 del Collegio di Bologna;

- le operazioni sono state eseguite regolarmente non si evidenziano anomalie e sono regolate dall'art. 24 del d.lgs. 11/2010 che stabilisce: “.3. Il prestatore di servizi di pagamento è responsabile solo dell'esecuzione dell'operazione di pagamento in conformità con l'identificativo unico fornito dall'utente anche qualora quest'ultimo abbia fornito al suo prestatore di servizi di pagamento informazioni ulteriori rispetto all'identificativo unico”;
- appare provata la colpa grave della ricorrente in quanto le operazioni sono state inserite ed autorizzate direttamente dallo stesso attraverso l'utilizzo degli strumenti normalmente utilizzati per eseguire transazioni tramite il canale mobile della banca, canale PSD2 e SCA compliant in quanto per la disposizione dell'operazione contestata sono stati utilizzati: 1) Il telefono della Ricorrente (possesso) 2) L'App Mobile Banking (possesso) 3) Il codice PIN per l'accesso all'App Mobile Banking (conoscenza) 4) Il codice Mpin (MobileCode) per l'autorizzazione della disposizione (conoscenza) tutte credenziale di esclusiva conoscenza/possesso di parte ricorrente;
- quanto accaduto è riconducibile ad un classico caso di vishing, si richiama in proposito la decisione del collegio di Bologna n 18714/20 “La ravvisata assenza di cautela dell'utente appare difficilmente scusabile, trattandosi in tal caso di un fenomeno oramai diffusamente noto, che quanto meno qualunque utente dotato di normale avvedutezza e prudenza deve essere in grado di individuare, non facendosi trarre in inganno. “Nell'ipotesi del “phishing tradizionale”, il cliente è, pertanto, vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di “accalappiamento” possono dirsi ormai note al pur non espertissimo navigatore di internet” (cfr. Collegio di Bologna, decisione n. 4585 del 2018); così anche la decisione n.14/20 sempre del collegio di Bologna “L'orientamento dei Collegi ABF è nel senso di ravvisare la colpa grave del cliente qualora risulti che quest'ultimo abbia comunicato a terzi i dati associati ad uno strumento di pagamento in risposta ad una e-mail di phishing ovvero SMS”;
- in relazione alla strong authentication, si riporta un estratto della decisione n. 4775/21 del 23.02.2021, Collegio di Bologna “...Orbene, in linea con l'orientamento del sistema ABF alla luce dei recenti sviluppi normativi sulla materia, per decidere questo ricorso il Collegio procede, in primis, a verificare la conformità delle operazioni ai nuovi standard in materia di Strong Consumer Authentication- SCA (art. 10bis del medesimo D.Lgs. n. 11/2010). In particolare, l'art. 1, lettera qbis del medesimo decreto chiarisce, conformemente alla suddetta direttiva, che la c.d. autenticazione forte consiste in “un'autenticazione basata sull'uso di due o piu' 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, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione”. Sul punto, è intervenuta l'EBA con le “Opinion” del 21 giugno 2019, nelle quali sono stati passati in rassegna alcuni dei più comuni sistemi di autenticazione predisposti dagli intermediari per valutare se possano o meno annoverarsi tra i presidi di autenticazione forte, annoverando una lista di requisiti tecnici, compliant o non compliant con la SCA, ovvero: 1) elementi di “Inherence: something the user is”, 2) elementi di “Possession: something only the user possesses”; 3) elementi di “Knowledge: something only the user knows”. Quindi, per questo Collegio occorre verificare innanzitutto se, nel caso di specie, l'operazione contestata sia stata autenticata mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d.
- “autenticazione forte”, appartenenti, in ogni caso, a due liste diverse (cfr. EBA-Op-2018-04, 13 June 2018).
- rileva anche la decisione n. 3569 dell'8 aprile 2025 del Collegio di Palermo in merito al consenso della ricorrente nell'effettuazione dell'operazione: “irrilevante che il consenso fosse stato viziato dal raggio dei truffatori, dal momento che un consenso viziato pur sempre un consenso, secondo le

categorie del diritto civile (tant'è che il codice prevede, per le ipotesi appunto di vizio del consenso, il rimedio, costitutivo, dell'annullamento, escludendo invece la nullità radicale del negozio)".

- richiama infine la sentenza della Cassazione Civile 13 marzo 2023, n. 7214 che ha rilevato in caso di phishing la condotta imprudente e negligente del correntista, esprimendosi in merito al tema della responsabilità del cliente che sia rimasto vittima di una frode informatica (phishing) e stabilendo che il comportamento del titolare del conto è da considerarsi "imprudente e negligente" in quanto il cliente ha fornito i propri codici personali (richiestigli con una telefonata fraudolenta) consentendo così al truffatore di utilizzarli successivamente per effettuare disposizioni di pagamento; pertanto, chiede che il ricorso sia respinto per le motivazioni esposte e alla luce degli orientamenti favorevoli in materia (cfr. decisioni N. 1341/21 e 17867/21 del Collegio di Roma e la decisione n. 21437/20 del Collegio di Palermo).

DIRITTO

1.- La controversia ha ad oggetto n. 3 bonifici come dettagliati di seguito per un importo complessivo di € 4.007,43 (comprese le commissioni).

L'operazione contestata è stata effettuata sotto la vigenza del d.lgs. 11/2010, come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2).

2.- La parte ricorrente dichiara che il 28/01/2025, alle ore 15:48, ha ricevuto sul proprio telefono cellulare un SMS apparentemente proveniente dalla banca che lo informava di un accesso eseguito da un nuovo dispositivo telefonico e lo invitava a chiamare il servizio assistenza ad un numero di cellulare. Allarmato dal messaggio ricevuto, chiamava il numero indicato al quale rispondeva una persona che si qualificava come operatore dell'ufficio antifrode e lo induceva a disporre tre bonifici.

3.- Il ricorrente produce copia del messaggio e del registro chiamate, che sono state registrate come "sospetto spam".

Dall'esame del messaggio esca (e di quelli successivi) emerge che non si evincono nella chat messaggi genuini. Per cui la chat sia pur intestata all'intermediario appare poco attendibile. Inoltre, vi sono ulteriori indici di inattendibilità come, ad esempio, il tono del messaggio e, soprattutto, l'indicazione di un numero mobile da chiamare quale numero dell'assistenza.

Peraltro, anche il registro delle chiamate evidenzia come le stesse (effettuate verso un numero mobile) siano state contrassegnate come "Sospetto spam".

4.- Nel caso di specie il ricorrente ammette di aver eseguito materialmente le operazioni indicate al telefono dal truffatore.

L'orientamento unanime dei Collegi territoriali ritiene che, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2. Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura").

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 come, ad esempio, nei casi di:

- mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;
- mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore;

- mancato rilievo di indici di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.

Laddove quindi emerga che è lo stesso ricorrente ad aver materialmente disposto l'operazione contestata, come nel caso di specie considerata l'ammissione della ricorrente, i Collegi ABF ritengono inapplicabile la disciplina prevista dal d.lgs. n. 11/2010, rigettando la domanda di restituzione dell'importo dell'operazione involontariamente disposta (Collegio di Roma, decisione n. 1314/2024).

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE