

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) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 09/01/2026

FATTO

La parte ricorrente espone quanto segue.

- in data 23.04.2025 alle 13:50 riceveva un sms da un numero riferibile alla resistente con il quale veniva invitata ad aggiornare un questionario antiriciclaggio tramite un link;
- cliccava sul link e veniva reindirizzata su una pagina web identica a quella della banca e inseriva le credenziali per accedere all'home banking;
- alle 00:48 del 25.04.2025 riceveva una e-mail che la informava del cambio della mail e del telefono collegati al conto, ma tali modifiche non erano state da lei autorizzate;
- contattava il numero verde e apprendeva che dal conto erano stati prelevati tra il giorno 25/04/2025 e il 26/04/2025 euro 1.325,50, di cui chiede il rimborso.

L'Intermediario eccepisce quanto segue:

- risulta che alle ore 15:15 del 23 aprile 2025, due giorni prima che venisse autorizzata la prima delle operazioni contestate (ossia l'operazione delle ore 1:02 del 25 aprile 2025), sia stata installata l'APP su un altro dispositivo (il device del frodatore) tramite inserimento dei dati personali della Cliente (Codice Cliente, Data di nascita, Codice PIN) e successivo inserimento del codice OTP ricevuto sul numero di cellulare censito in anagrafica;
 - l'installazione della app è stata possibile grazie alla cooperazione fornita dalla ricorrente al frodatore.
- In generale, l'installazione della APP su device di altro soggetto avviene tramite SCA attraverso i seguenti passaggi:

1. accesso tramite app sul nuovo dispositivo con l'inserimento del Codice Cliente, data di nascita e Codice PIN – elemento di conoscenza;
 2. invio di un sms OTP sul recapito telefonico registrato (elemento di possesso);
 3. l'inserimento in app dell'OTP ricevuto;
- in assenza della comunicazione delle credenziali, nonché del codice OTP, l'operatività disconosciuta non avrebbe potuto realizzarsi;
 - alle ore 15:15 è stata, pertanto, consentita l'installazione dell'APP sul device del frodatore, segnalato da apposita e-mail di alert;
 - hanno poi fatto seguito in data 25 aprile 2025 le modifiche all'indirizzo email e al numero di telefono della Cliente e l'autorizzazione di tutte le transazioni successive;
 - chiarito ciò, dalle verifiche condotte risulta che le operazioni disconosciute siano state correttamente autorizzate tramite autenticazione forte;
 - l'attivazione dell'app, la modifica dell'indirizzo e-mail e del numero di telefono e le operazioni sono state eseguite in orari e in date differenti, e in detto arco temporale la cliente avrebbe dovuto attivarsi tempestivamente per interrompere l'iter criminoso in corso.

Chiede di rigettare il ricorso in quanto infondato.

Con le repliche la parte ricorrente rileva quanto segue:

- la nuova APP è stata attivata a seguito di un sms che risultava provenire dalla banca e che riportava una richiesta di aggiornamento del questionario antiriciclaggio;
- inoltre, le notifiche alert sono state inviate ad un indirizzo e-mail sconosciuto;
- di fatto la notifica di cambio dell'indirizzo e-mail è arrivata solo alle ore 00:48 del 25/04/2025, come anche il messaggio di cambio del cellulare, rendendo di fatto impossibile rendersi conto delle operazioni in corso se non la mattina del 25/04/2025;
- è stato impossibile prendere contatto con il servizio clienti, considerando che il 25 aprile è un giorno di festa;
- seppur chiaro a posteriori che l'sms era parte di una frode, lo stesso era in coda a messaggi genuini della resistente.

DIRITTO

Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 25 e 26 aprile 2025. Risultano pertanto effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tale operazione è altresì successiva alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-ter, 5-quater e 10-bis del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 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. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.

Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame. In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove

quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-bis, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "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. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-bis), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più 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".

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

La ricorrente chiede il rimborso di una serie di operazioni eseguite tra il 25 e il 26 aprile 2025 per un totale di 1.325,50 euro.

Come eccepito dall'intermediario, l'importo richiesto non coincide con l'importo delle operazioni contestate nel modulo di riconoscimento.

L'intermediario afferma di considerare solo i bonifici in uscita, la cui somma è superiore all'importo richiesto dalla ricorrente: bonifico ordinario del 25 aprile 2025 di euro 550,00; bonifico ordinario del 25 aprile 2025 di euro 19,00; bonifico ordinario del 25 aprile 2025 di euro 3,00; bonifico ordinario del 25 aprile 2025 di euro 0,50; bonifico istantaneo del 26 aprile 2025 di euro 1.310,00; totale 1.882,5 euro (a fronte di un importo richiesto di 1.325,50 euro).

Si analizzeranno quindi i bonifici in uscita sottolineando che, ai fini dell'eventuale quantum da restituire, la richiesta della ricorrente è di 1.325,50 euro (ex art. 112 c.p.c.).

L'intermediario rappresenta che le operazioni sono state eseguite tramite il device utilizzato dai frodatori dopo che gli stessi frodatori hanno installato la app con le credenziali fornite dalla ricorrente. In particolare, l'intermediario precisa che alle ore 15:15 del 23 aprile 2025 è stata installata l'APP sul dispositivo dei frodatori tramite inserimento dei dati personali della cliente (Codice Cliente, Data di nascita, Codice PIN) e codice OTP ricevuto sul numero di cellulare censito in anagrafica dalla Cliente (rectius 347***936).

A seguito della installazione della app i frodatori hanno poi configurato lo smartcode.

Il numero di telefono è quello indicato in denuncia.

Alle ore 15:15 è stato inviato apposito alert mediante notifica a mezzo email; hanno poi fatto seguito in data 25 aprile 2025 le modifiche dell'indirizzo email e del numero di telefono della ricorrente.

Con riguardo all'esecuzione delle operazioni l'intermediario riferisce che:

- alle ore 01:01:11 del 25 aprile 2025 si è registrato l'accesso alla APP (possesso) digitando il Codice Segreto (SmartCode – conoscenza);
- i pagamenti in contestazione sono stati poi eseguiti tramite inserimento dello stesso Smartcode (conoscenza) in app (possesso).

Vengono prodotte le tracciate relative al bonifico ordinario da 550,00 euro del 25 aprile 2025 e del bonifico istantaneo da 1.310,00 del 26 aprile 2025.

L'intermediario fornisce evidenza della email di alert inviate in corrispondenza dei bonifici in esame ma verosimilmente sono state recapitate all'indirizzo email modificato dai truffatori.

In conclusione, l'installazione dalla app sul device dei frodatori è stata effettuata mediante inserimento del Pin (conoscenza) e della OTP (possesso).

L'esecuzione della operazione è stata effettuata mediante inserimento dello smartcode (conoscenza) sulla app installata sul device dei frodatori (possesso).

La parte ricorrente afferma di aver ricevuto in data 23.04.2025 alle 13:50 un sms da un numero riferibile alla resistente tramite il quale veniva invitata ad aggiornare un questionario antiriciclaggio tramite un link.

Ammette di aver cliccato sul link e inserito in una pagina fake della banca le credenziali per accedere all'home banking.

Non fornisce ulteriori dettagli relativi alla frode ma riferisce che il 25 aprile avrebbe ricevuto le mail che l'avvisavano del cambio di e-mail e del numero di telefono collegati al suo conto e che solo dopo essere riuscita a contattare il servizio clienti scopriva delle operazioni in contestazione.

Il messaggio truffaldino risulta inserito in una chat, contenente messaggi genuini, che riporta come mittente la resistente; non presenta errori grammaticali ma il link non contiene riferimenti alla resistente; nella stessa chat risultano anche il messaggio del 23 aprile 2025 con l'OTP per installare la app su un altro device, nonché il messaggio di alert di modifica dell'indirizzo email avvenuto il 25 aprile 2025.

L'intermediario fornisce evidenza di aver inviato la email di alert che segnalava la installazione della app su un nuovo device. Inoltre, la stessa ricorrente fornisce evidenza di aver ricevuto l'sms con la OTP per installare la app su un altro device.

Le email e gli sms relativi all'operatività fraudolenta del 25 e 26 aprile sono stati verosimilmente inviati sulla email e il cellulare modificati dai frodatori.

Nel modulo di disconoscimento si legge che la ricorrente avrebbe tentato di contattare il servizio clienti il 25 aprile, dopo aver presentato anche la denuncia (che risulta presentata il 25 aprile 2025) ma di non esservi riuscita se non il 28 aprile 2025.

Ciò risulta confermato anche dalla circostanza che è in atti un primo reclamo della ricorrente del 25 aprile 2025.

L'intermediario al riguardo si limita ad affermare che la ricorrente avrebbe segnalato tardivamente l'accaduto.

Nel caso di specie, si tratta di ipotesi di *smishing* in cui il messaggio reca, quale mittente, la denominazione riferibile all'intermediario, tanto che il testo si è inserito nella visualizzazione dello smartphone all'interno della conversazione contenente messaggi genuini, effettivamente provenienti dall'intermediario (*spoofing*).

Tuttavia, si deve rilevare che, come eccepito dalla banca, il link non contiene alcun riferimento al nome della banca.

Secondo la più recente posizione condivisa da tutti i Collegi territoriali, nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, "a meno che non si rinvenano [...] indici di inattendibilità o anomalia del messaggio; in tale caso, potrà essere ravvisato un concorso di colpa tra le

parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario".

Pertanto, alla luce delle risultanze istruttorie, il Collegio ritiene che sussistano profili di colpa grave del cliente - consistente nell'aver dato seguito alle istruzioni del frodatore nonostante la capillare campagna informativa posta in essere dall'intermediario - e che essi siano tali da contribuire alla causazione dell'evento dannoso; tuttavia, ritiene altresì che la loro efficienza causale non sia esclusiva. Il caso di specie si discosta, infatti, dallo *smishing* perpetrato attraverso modalità tipiche e ampiamente note, dove la colpa grave del cliente è causa sufficiente dell'evento dannoso, in quanto capace di deviare la catena causale che collega il comportamento illecito del frodatore e il concretarsi della frode, assorbendo del tutto, così, il nesso di causalità.

Nel caso in esame, invece, il truffatore ha adottato un sistema tecnicamente più sofisticato, tale da concretare un'ipotesi di malfunzionamento del servizio di pagamento o altro inconveniente connesso al servizio di disposizione di ordine di pagamento, pur inteso in senso ampio, destinato a ricadere nella sfera del rischio di impresa dell'intermediario. Non è dubbio, infatti, che le operazioni siano un effetto di tale malfunzionamento, sul quale si innesta la colpa grave del cliente. Quest'ultima, però, a parere del Collegio, non è adeguata ad assorbire completamente il nesso di causalità, ma concorre con esso (Coll. Milano, dec. n. 2892/2021; Coll. Roma, dec. n. 1625/2022).

Alla luce di quanto sopra esposto il Collegio valuta il concorso tra le parti e liquida in via equitativa in favore del ricorrente a titolo risarcitorio l'importo di € 700,00.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 700,00, determinata in via equitativa.

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