

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) RUGGIERO	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO RUGGIERO

Seduta del 27/01/2026

FATTO

La ricorrente espone di essere stata vittima di una truffa (“*phishing*”); deduce, in particolare, di aver ricevuto un SMS il giorno 9.3.2025, apparentemente proveniente dall’intermediario, con cui le veniva segnalato l’avvenuta operazione di prelievo per € 3.000,00 e le veniva indicato un numero telefonico da contattare, per l’ipotesi in cui detta operazione non fosse stata autorizzata dal cliente.

Deduce di aver contattato l’utenza indicata e di aver appreso da un sedicente operatore dell’intermediario che il conto era stato “attaccato” da un virus informatico, sicchè si rendeva necessario eseguire una procedura per risolvere tale criticità.

Sennonchè, all’esito della procedura seguita riceveva una mail da parte della Banca che la informava dell’esecuzione di due addebiti, dell’importo totale di € 3.000,00.

Insoddisfatta dell’esito infruttuoso del reclamo, la ricorrente si è rivolta all’Arbitro, al quale ha chiesto il rimborso dell’importo sottratto ed ogni ulteriore provvedimento in suo favore.

Costituito nel procedimento, l’intermediario ha contestato le domande della ricorrente, rilevando preliminarmente che la cliente ha autorizzato personalmente i prelievi *cardless* in questione con il proprio *device* certificato e che, per tale ragione, la richiesta di rimborso non rientra nell’ambito di applicazione di cui al d. lgs. n. 11/2010, dal momento che i prelievi sono stati eseguiti con il consenso

del titolare dello strumento di pagamento, sebbene sulla base di un consenso viziato dagli artifici e raggiri posti in essere da un truffatore.

Ha precisato che il prelievo *cardless* permette di prelevare somme di denaro dalle casse automatiche della Banca senza usare la carta, ma solo con il *device* certificato; a tal fine è necessario inquadrare con lo *smartphone* il “QR code” visibile sull’ATM e attendere che l’*App* si colleghi automaticamente alla cassa; quindi, dopo aver selezionato l’importo e autorizzato con il PIN l’operazione, il denaro viene erogato.

Ciò precisato, il resistente ha rilevato che dalle tracciatore dei movimenti informatici emerge che le operazioni disconosciute sono state correttamente disposte ed eseguite dopo essere state “*autenticate, correttamente registrate e contabilizzate*”, senza aver “*subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*”.

L’intermediario ha chiarito inoltre che i due prelievi delle ore 16:19 e 16:21 sono stati regolarmente disposti e contabilizzati a valere sul conto corrente intestato alla ricorrente.

Ne consegue che le operazioni risultano correttamente autenticate dal *device* della cliente, rispettando i requisiti della “Conoscenza” e del “Possesso”.

Nel caso in esame, in sede di denuncia, la cliente ha peraltro dichiarato che sia l’SMS ricevuto che l’utenza telefonica contattata non sarebbero in alcun modo riferibili alla banca.

Parte resistente ha altresì eccepito che l’ SMS prodotto presenta evidenti elementi di anomalia che ne escludono l’autenticità e la riconducibilità alla banca: in particolare, il numero del mittente non risulta in alcun modo associabile ai canali ufficiali dell’istituto di credito, trattandosi di un’utenza mobile generica e non di un numero verificato o collegabile all’istituto. Inoltre, il testo del messaggio è redatto in forma approssimativa e incoerente rispetto agli standard comunicativi di un ente bancario, con assenza di riferimento personalizzato al destinatario, con utilizzo di toni allarmistici e inclini all’immediata azione ne compromette poi ulteriormente la credibilità.

Inoltre, l’utenza indicata nel messaggio telefonico non risulta riconducibile ai recapiti ufficiali della banca, il che conferma ulteriormente la natura sospetta della comunicazione.

L’intermediario ha sottolineato la lacunosità nella ricostruzione dell’accaduto da parte della ricorrente, dal momento che nulla viene riferito in relazione alla scansione del QR-code, attività necessaria per il buon fine dei prelievi; dal che si può verosimilmente supporre che la ricorrente, inquadrando con il proprio *device* certificato i QR code inviati su di un secondo *device* dai truffatori che si trovavano davanti all’ATM, abbia consentito l’erogazione del denaro.

L’intermediario ha rilevato infine di aver fornito alla propria clientela ampia informativa sul proprio sito internet circa i pericoli connessi alle frodi informatiche e istruisce con attenzione i clienti riguardo le diverse tipologie delle stesse, nonché gli strumenti da adottare per evitare possibili danni.

Secondo quanto statuito dai recenti orientamenti arbitrali, al momento in cui sono state effettuate le operazioni di prelievo non sussisteva - e tutt’ora non sussiste – l’obbligo in capo all’intermediario di procedere a un monitoraggio in tempo reale o a un “blocco automatico” delle operazioni.

L’intermediario ha chiesto quindi il rigetto del ricorso.

DIRITTO

La questione sottoposta all’Arbitro concerne la richiesta di rimborso relativa a due operazioni disconosciute dalla ricorrente, consistenti in prelievi *cardless* autorizzati *online* con l’utilizzo di credenziali a lei riferibili, per l’importo complessivo di € 3.000,00. In particolare, si tratta di due

operazioni eseguite entrambe il 9.3.2025, di cui la prima di € 2.000,00 e la seconda di € 1.000,00.

L'istante ha reso la relativa denuncia presso l'Autorità competente il 10.3.2025, depositata in atti; ha prodotto il messaggio telefonico ricevuto, mentre non ha fornito evidenza dello *screenshot* della telefonata ricevuta.

Dalla narrazione attorea, emerge che le due operazioni di prelievo presso ATM, eseguite in modalità "*cardless*" (ovvero senza la presenza fisica della carta), sono state "iniziate" dal truffatore che ha inviato alla ricorrente i *QRcode* visualizzati sull'ATM; la ricorrente, quindi, utilizzando l'*app* installata sul suo *device*, ha inquadrato i predetti codici, ha selezionato l'importo da prelevare e ha inserito il PIN per autorizzare i prelievi.

Le operazioni contestate sono state quindi autorizzate dal *device* associato al profilo della ricorrente; in particolare, l'accesso e i pagamenti disconosciuti sono stati autorizzati con sistema di autenticazione a due fattori (SCA) mediante *device* certificato e inserimento del PIN, mentre l'innalzamento dei limiti operativi eseguito prima delle operazioni disconosciute ha richiesto anche l'inserimento di un codice OTS inviato al numero di telefono certificato della ricorrente.

Ciò premesso, in punto di fatto, occorre osservare che la controversia è disciplinata dal d.lgs. n. 11/2010, di attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno (c.d. PSD), come modificato dal d.lgs. n. 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). In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del d. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e risultano recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA.

Per quanto riguarda l'onere della prova, l'art. 10, d. lgs. 11/2010, come modificato dal d.lgs. 15/12/2017, n. 218, richiede che il prestatore di servizi di pagamento fornisca la prova dell'autenticazione, della corretta registrazione e della contabilizzazione dell'operazione di pagamento effettuata, oltre che la prova del mancato malfunzionamento delle procedure necessarie per la sua esecuzione del pagamento medesimo. Solo nel caso in cui la resistente abbia offerto la prova dell'autenticazione delle transazioni disconosciute, le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento circa la colpa grave del ricorrente medesimo.

La norma in questione è diretta a porre in modo esplicito l'onere della prova a carico del PSP ed è contenuta in un complesso di norme (quelle del decreto legislativo n. 218/2017) volte ad introdurre nella legge che regola la materia dei servizi di pagamento disposizioni rafforzative del "*regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori*". Ed in effetti, la nuova disposizione sull'onere probatorio, di cui al comma 2 dell'art. 10, va a potenziare la tutela dell'utente il quale, nell'utilizzo degli strumenti di pagamento, può restare vittima di attività fraudolente che, allo stato delle conoscenze tecnologiche, possono prevalere sui presidi di sicurezza approntati dal PSP, senza che al comportamento dell'utilizzatore possa riconoscersi alcuna efficienza causale (o quanto meno non determinante) nella produzione del fatto illecito.

Orbene, l'intermediario ha depositato le tracciate descritte anche nelle controdeduzioni; ha depositato l'evidenza dell'OTS inviato al numero di telefono certificato della ricorrente e necessario per autorizzare l'innalzamento dei limiti operativi.

Nel caso di specie, l'operatività contestata consiste in due prelievi *cardless* dell'importo di € 2.000,00 e di € 1.000,00, eseguiti nell'arco di un minuto e pochi minuti dopo l'innalzamento dei limiti di prelievo già stabiliti.

Con riferimento al servizio di SMS *alert*, la banca ha inviato alla cliente un *alert* successivo alle singole operazioni a mezzo mail, che tra l'altro la ricorrente avrebbe visionato subito dopo le operazioni contestate (eseguite nell'arco di un minuto).

Tuttavia, con riferimento al messaggio civetta ricevuto dalla ricorrente e depositato, lo stesso non presenta indici di riconducibilità all'intermediario, sia quanto al numero del mittente non associabile ai canali della banca, sia quanto al testo redatto in modo approssimativo e in modo difforme dagli standard di comunicazione con la clientela, sia ancora per le modalità dei toni allarmistici che ne compromettono la credibilità.

Orbene, alla luce della descrizione del procedimento di autenticazione e di autorizzazione, confortato dalle allegazioni dei log e delle schermate prodotte dall'intermediario il sistema approntato dall'intermediario sembra idonea a garantire la SCA e non sembra potersi desumere che lo stesso abbia disatteso gli obblighi di sicurezza posti a suo carico; di contro, alla luce della documentazione prodotta, risulta la prova, in via presuntiva, della colpa grave dell'utente, secondo quanto indicato nella decisione del Collegio di Coordinamento n. 22745/2019, avendo questi consentito con il proprio comportamento il determinarsi della truffa subita, con ingenua ed imprudente adesione alle istruzioni impartite dai malfattori.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE