Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) SCIBETTA	Membro di designazione rappresentativa degli intermediari
(PA) CLEMENTE RUIZ	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MELI

Seduta del 06/02/2025

FATTO

Con ricorso pervenuto il 12.11.2024, la ricorrente espone che in data 23.05.2024 riceveva sul proprio telefono cellulare delle comunicazioni apparentemente provenienti dall'intermediario, che la invitavano ad accedere al proprio *home banking* per delle anomalie. Riceveva quindi una chiamata da parte di un numero di telefono apparentemente riconducibile ad un centro operativo per la sicurezza cibernetica delle forze dell'ordine. Attraverso l'utilizzo fraudolento della carta legata al conto intrattenuto con l'intermediario venivano, dunque, effettuati tre bonifici e due operazioni di pagamento, per un totale di € 11.870,00. Pertanto, la ricorrente, pur avendo adottato l'ordinaria diligenza del buon padre di famiglia, non ha potuto rilevare la frode attuata dai malviventi, in ragione dei mezzi utilizzati. Inoltre, poiché l'operatività contestata non era in linea con le abitudini del cliente, l'intermediario avrebbe dovuto predisporre un sistema di monitoraggio tale da intercettare tali anomalie. L'intermediario non ha inviato né un codice OTP autorizzativo, né un sms alert, che avrebbe permesso alla cliente di chiedere tempestivamente il blocco della carta.
La ricorrente chiede di accertare il proprio diritto al rimborso della somma sottratta e, in subordine, nel caso fossero ravvisato anche profili di propria responsabilità, di limitare il diritto al rimborso nei limiti di cui all'art. 12, c. 3, d.lgs. n. 11/10, come modificato dal d.lgs. n. 218/17, di attuazione della direttiva 2015/2366/EU (PASD 2).

Con le controdeduzioni, l'intermediario chiede il rigetto del ricorso.
Sostiene che le operazioni disconosciute sono state correttamente autorizzate mediante l'utilizzo di credenziali statiche e dinamiche in possesso della cliente e correttamente registrate e contabilizzate, senza che si siano registrati malfunzionamenti. In particolare, gli accessi all'area riservata sono stati registrati dal dispositivo abituale, con riconoscimento biometrico. Le operazioni di bonifico sono state autorizzate mediante l'inserimento di OTP ricevuto sul numero di cellulare della cliente univocamente associato al conto, previo accesso all'area riservata con modalità che vengono descritte. Per quanto concerne le operazioni di pagamento tramite carta, le stesse sono state autorizzate mediante l'inserimento dei dati statica della carta (PAN, data di scadenza), nonché del CVV dinamico appositamente generato e l'inserimento dell'OTP ai fini del rispetto dell'autenticazione forte. I log prodotti dimostrano la corretta autenticazione delle operazioni, nonché la collaborazione di parte ricorrente al disegno fraudolento. Dalla dinamica della frode emerge la colpa grave della cliente che, come esplicitamente ammesso, ha fornito username, password e dati della carta ad un sedicente operatore di un altro intermediario. La ricorrente, inoltre, ha riferito di aver ricevuto la telefonata da un numero di cellulare. Nonostante ciò, parte resistente, dopo essere stata avvertita della truffa, si è subito prodigata per il recupero delle somme oggetto dei bonifici, e in data 16.07.2024, ha restituito € 5.985,15, come può evincersi da evidenza allegata alle controdeduzioni.
Con la replica e la controreplica, le parti hanno sostanzialmente confermato le rispettive posizioni.

DIRITTO

La controversia verte sulla richiesta di rimborso di somme oggetto di bonifici e operazioni di pagamento che la ricorrente nega di avere autorizzato.
Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del dlgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e 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 (v. in particolare il parere dell'EBA del 21 giugno 2019).
Nel caso di specie, la contestazione riguarda tre bonifici e due operazioni di pagamento con carta, tutti effettuati in data 23.05.2024. Dalle evidenze prodotte dall'intermediario, risulta che le operazioni cointestate sono le seguenti:
1. Operazione di pagamento di € 1.900,00, alle ore 12:53:00;
2. Operazione di pagamento di € 1.070,00, alle ore 13:10:06;
3. Bonifico di € 3.000,00, alle ore 13:22:11;
4. Bonifico di € 3.000,00, alle ore 13:28:24;
5. Bonifico di € 2.970,00, alle ore 13:31:08.

L'importo totale delle operazioni è, dunque, di € 11.940,00. La ricorrente chiede però € 11.870,00 e, con le repliche, nulla dice sul punto. E', dunque, quest'ultima la somma che

sarà considerata nell'esame del ricorso. A tale proposito, va però aggiunto che la resistente, una volta messa al corrente della truffa, si è attivata per il recupero delle somme, e ha disposto in data 16.07.2024 un accredito alla cliente di € 5.985,15. Circostanza, questa, che la ricorrente ha confermato. Oggetto della domanda rimangono, pertanto, i residui € 5.884,85. Si deve, peraltro, precisare che le somme recuperate e rimborsate riguardato specificamente i bonifici. Ne deriva che, alla luce del rimborso effettuato, la pretesa deve ripartirsi tra le diverse operazioni in questa misura:
- Operazioni di pagamento: resta impregiudicata la domanda di € 2.970,00;
- Bonifici: la domanda risulta automaticamente ridotta a € 2.914,85.

In merito alle circostanze della frode, dalla denuncia presentata ai Carabinieri il 24.05.2024, emerge quanto segue. In data 23.05.2024 la ricorrente veniva contattata sulla sua utenza cellulare da un sedicente operatore, che si occupava di servizi antifrode, incaricato dall'intermediario *Alfa*. Questi la informava di un attacco hacker e che le somme conservate nel conto n. ***, intrattenuto con lo stesso intermediario, erano in pericolo. Appurata la presenza di movimenti effettivamente sconosciuti, la ricorrente si persuadeva della buona fede dell'interlocutore, e gli forniva i dati di accesso all'anzidetto conto. Il truffatore, successivamente, chiedeva anche le credenziali per poter accedere al conto detenuto presso parte resistente. A tale richiesta la ricorrente rispondeva fornendo *username*, *password*, numero di carta, scadenza e codice CVV. Lo stesso interlocutore convinceva poi la ricorrente ad "accettare" tre operazioni di bonifico, al fine di stornare le operazioni anomale. Ancora, venivano effettuati altri due pagamenti, di € 1.070,00 ed € 1.900,00. In seguito, il truffatore persuadeva la ricorrente a disporre ulteriori operazioni fraudolente attraverso il conto intrattenuto con l'intermediario *Beta*. Solo di fronte alla richiesta di utilizzare i fondi intrattenuti presso un ulteriore intermediario la ricorrente rifiutava di seguire le istruzioni fornite, nonostante l'intervento di un fantomatico ufficiale delle forze dell'ordine.

Si deve, in via preliminare, accertare se la ricorrente abbia autorizzato personalmente e integralmente le operazioni, sia pure dietro l'indicazione dei truffatori (come sostenuto dall'intermediario). Com'è noto, infatti, secondo orientamento uniforme dei Collegi territoriali, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, personalmente autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP. Quando, invece, 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") (si veda, ad es., Collegio di Palermo, dec. n. 2787/24).

Dall'esposizione dei fatti sorge il dubbio che la cliente abbia personalmente effettuato (cioè integralmente disposto) almeno i due pagamenti di € 1.070,00 e 1.900,00 ("*mi veniva richiesto di effettuare altri due pagamenti*"), sia pure su indicazione dei truffatori. In realtà, l'espressione resta ambigua, potrebbe anche essere intesa nel senso che il soggetto dell'"*effettuare*" riguardi il richiedente (cioè il truffatore). Decisivo è, poi, il fatto che la ricorrente riferisca di avere fornito *username*, *password*, numero di carta, scadenza e codice CVV: tutte informazioni che non sarebbero state necessarie al truffatore, laddove questo si fosse limitato ad indurre la ricorrente ad effettuare essa stessa le operazioni. Anche ai due pagamenti si devono, dunque, applicare le disposizioni derivanti dalla PSD2.

Si deve, pertanto, procedere alla verifica della conformità alla SCA del sistema descritto da parte resistente.
L'intermediario afferma che l'altro fattore utilizzato per autorizzare le operazioni in oggetto è stato l'OTP sms (elemento di possesso), qualificando il CVV dinamico come elemento di conoscenza.
In realtà, il fattore di autenticazione rappresentato dal CVV dinamico, secondo le indicazioni fornite dall'EBA nell'Opinion del 21 giugno 2019, è identificato anch'esso come elemento di possesso. Come già deciso in casi analoghi dai Collegi territoriali, non può ritenersi conforme alla SCA un sistema basato su due elementi di possesso, richiedendosi il ricorso ad almeno due fattori di autenticazione appartenenti a categorie diverse (si vedano Collegio di Palermo, dec. n. 12152/2024 e 12156/2024; Collegio di Napoli, dec. n. 6180/24, Collegio di Torino, dec. nn. 5255/24 e 7207/24; Collegio di Bari, dec. n. 9345/23; Collegio di Roma, dec. n. 2840/23 e n. 10679/23).
Ne deriva che, mancando la prova della conformità alla SCA, i due pagamenti devono essere rimborsati, senza procedersi ad ulteriori valutazioni.
Per quanto riguarda i bonifici, la cliente afferma: "*mi veniva richiesto di accettare dal mio dispositivo tre operazioni (…) a seguito di bonifici che effettuavo contestualmente*". Nel caso di specie, non è chiaro se tali disposizioni siano state solo confermate dalla cliente, ma predisposte dai malfattori, o invece integralmente eseguite dalla cliente. Il dubbio non è però sufficiente ad affermare senz'altro la circostanza che renderebbe inapplicabile la specifica normativa, e si deve pertanto procedere con l'esame del merito della questione, partendo dall'accertamento della conformità alla SCA.
Dalle dichiarazioni e dalle evidenze fornite dell'intermediario, emerge che l'esecuzione delle operazioni richiede l'accesso all'area riservata del cliente. Ciò può avvenire via web, e, a tal fine, è necessario inserire le credenziali (*username* e *password*), o via app. In questo caso, si accede con il meccanismo di sblocco biometrico dello smartphone impiegato, che dovrà essere attivato previo accesso all'area riservata (con *username* e *password*) e compiendo, poi, i seguenti passaggi:
- entrata nelle impostazioni "Modalità di accesso/firma";
- clic su "Accesso con dati biometrici";
- inserimento dell'OTP ricevuta al numero di cellulare indicato dal cliente al momento dell'apertura del rapporto e univocamente associato ad esso.

Dopo l'accesso all'area riservata, per eseguire un bonifico è necessario:
- entrare nel Conto e cliccare su "Bonifici/Giroconti";
- inserire un nuovo beneficiario o sceglierlo tra i contatti precedentemente salvati;
- scegliere la topologia di bonifico e indicare la causale;
- confermare l'ordine di bonifico mediante inserimento dell'OTP ricevuta al numero di cellulare indicato dal cliente al momento dell'apertura del rapporto e univocamente associato ad esso.

Dunque, ai fini della SCA, l'accesso all'area riservata rappresenta il fattore di conoscenza e l'OTP quello di possesso.
Venendo alle evidenze sull'esistenza ed il funzionamento di tale sistema, l'intermediario afferma che tutti gli accessi e le operazioni sono state poste in essere mediante dispositivo attivato nei giorni 08.05.2024 – 09.05.2024, come può desumersi dai log prodotti. In particolare, tale dispositivo sarebbe stato attivato tramite autenticazione forte mediante inserimento di username e password e del codice OTP ricevuto al numero di telefono univocamente associato al conto. Successivamente, sulla base della legenda prodotta, risulta essere stato attivato sul dispositivo il fattore biometrico come fattore di autenticazione e viene fornita evidenza degli OTP inviati.

La conformità alla SCA si deve, dunque, ritenere provata e si può procedere alla valutazione di eventuali profili di colpa grave della ricorrente.
Dalle circostanze da essa riferite, elle ha ricevuto delle chiamate che, dagli *screenshot* prodotti, risultano provenire da numeri mobili, pacificamente non riconducibili all'intermediario. Ha pure ricevuto degli SMS il cui contenuto è caratterizzato da diverse sgrammaticature.
La chiamata dal sedicente esponente delle forze dell'ordine appare provenire da un numero che corrisponde a quello del Centro Operativo per la Sicurezza Cibernetica. Essa però è successiva al compimento delle operazioni disconosciute.
La stessa ricorrente ammette di avere accettato dal proprio dispositivo tre operazioni di bonifico a favore di un soggetto che le era stato indicato come "operatore della tesoreria dello stato" che si era preso in carico la sua pratica.
Deve, dunque, ritenere che il comportamento della ricorrente si sia caratterizzato per una grave mancanza di cautela, dovendo ormai essere noto a chi utilizza strumento elettronici di pagamento che la propria condotta rispetto a chiamate provenienti da sedicenti operatori degli intermediari debba essere improntata a estrema diffidenza, dovendosi procedere alla personale verifica con il servizio clienti, autonomamente contattato.
Dagli atti si ricava, tuttavia, come non fosse attivo alcun sistema di SMS *alert*. Se si considera che tra la prima operazione di pagamento e la seconda sono intercorsi circa otto minuti e che il primo bonifico è stato effettuato dopo venti minuti, sempre dalla prima operazione di pagamento, laddove fosse stato attivo un sistema di *alert*, questo avrebbe potuto richiamare l'attenzione della cliente sulla effettiva natura delle operazioni effettuate, consentendo di attivarsi per impedire il compimento di quelle ulteriori.
Per tali ragioni, il Collegio ritiene che anche l'importo delle tre operazioni di bonifico debba essere rimborsato, nei limiti di € 2.914,00.

PER QUESTI MOTIVI

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 5.884,85, oltre interessi legali dalla data del reclamo.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI