Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) PIERFRANCESCO BARTOLOMUCCI

Seduta del 11/11/2025

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che la controversia attenesse alla medesima truffa oggetto di un precedente ricorso, già deciso dal Collegio con una decisione di accoglimento, rimasta però inadempiuta dall'intermediario.
Faceva presente che in tale sede non avesse domandato il rimborso dell'operazione disconosciuta di importo pari ad € 990,00 in quanto l'intermediario aveva dichiarato che il reclamo per tale somma fosse stato accettato, salvo poi riaddebitare la somma in data 18/03/2025.
In considerazione dell'inadempimento dell'intermediario alla decisione n. **10/2025, relativa al precedente ricorso, riteneva che fosse necessario l'accoglimento di tale nuovo ricorso per proseguire la controversia per vie legali.
Chiedeva, pertanto, il rimborso dell'importo di ricorrente la somma di € 990,00.
Costituitosi ritualmente, l'intermediario rilevava che – in data 13/12/2024 – nel corso di una telefonata ricevuta da un sedicente operatore di altro intermediario tramite un numero di cellulare, venissero eseguiti due pagamenti (per € 990,00 ed € 2.000,00) con la carta di debito del ricorrente.
Sottolineava di aver proceduto al riaccredito "provvisionale" degli importi, e, dopo aver effettuato le verifiche del caso, di aver addebitato prima la somma di € 2.000,00 sul conto corrente e, dopo ulteriori verifiche e richieste da parte dell'esercente, anche la seconda somma di € 990,00, oggetto del presente ricorso.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Precisava che il cliente avesse presentato un ricorso relativamente al solo pagamento di € 2.000,00, ed avesse ottenuto la decisione favorevole n. **10/2025, alla quale, però, non aveva ritenuto di dare adempimento, in quanto il Collegio aveva ritenuto erroneamente che sia il CVV dinamico che la OTP rappresentino fattore di possesso.
Ricostruita nei riferiti termini la vicenda, rappresentava che l'operazione disconosciuta fosse stata correttamente autorizzata, con autenticazione forte a doppio fattori mediante CVV dinamico, fattore di conoscenza, e OTP, fattore di possesso, registrata e contabilizzata, in assenza di malfunzionamenti o anomalie.
Affermava, inoltre, che fossero state inviate tutte le notifiche *push* al cliente sia con riferimento all'autorizzazione del pagamento sia per informarlo dell'esecuzione di tale pagamento e del successivo blocco del conto.
Riteneva, dunque, che il cliente fosse stato vittima di *vishing*, ma poteva certamente essere individuata una colpa grave dello stesso, il quale aveva dato seguito ad una telefonata ricevuta da un numero di cellulare e alle richieste assurde del presunto operatore (di altro intermediario); soggiungeva che, come ammesso in denuncia, il cliente avesse seguito le indicazioni del truffatore, gli avesse comunicato i codici ricevuti via sms ed avesse autorizzato personalmente il pagamento oggetto del presente ricorso.
Riteneva che, verosimilmente, il cliente avesse inoltre fornito al sedicente operatore l'username ricevuto tramite sms, (parte del) PIN della carta visualizzato personalmente all'interno dell'app, l'OTP per generare il CVV dinamico della carta e il CVV dinamico della carta;
Considerava la truffa occorsa non particolarmente sofisticata, poiché non si sarebbe potuta concretizzare senza il negligente e colpevole apporto del cliente stesso.
Affermava di mettere a disposizioni dei propri clienti numerosi contenuti, in costante e continuo aggiornamento, in materia di sicurezza informatica, sia sul web sia tramite informative e-mail e in app.
Evidenziava, infine, che non avrebbe in alcun modo potuto impedire l'esecuzione dell'operazione contestata.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale riteneva che la truffa dovesse essere considerata come "particolarmente sofisticata" in quanto la chiamata proveniva dal numero ufficiale di assistenza dell'intermediario e che tale camuffamento fosse dipeso dalle insufficienti misure di sicurezza dei sistemi adottati dall'intermediario.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale evidenziava che il cliente avesse depositato le medesime repliche depositate per il precedente ricorso e che fossero, pertanto, non riferibili al presente ricorso.
Per il resto, richiama le difese già spiegate nei propri scritti difensivi.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione, successivamente disconosciuta.
In premessa, deve rilevarsi che la fattispecie sia stata già fatta oggetto di esame di una decisione da parte di questo Collegio, il quale ha già accertato – nel contesto della medesima truffa subita dal ricorrente – la responsabilità dell'intermediario in relazione ad un'altra operazione.
Dall'evidenza prodotta si rileva l'operazione contestata è stata effettuata in data 13/12/2024, il riaccredito provvisionale in data 18/12/2024 e il successivo storno in data 18/03/2025.
Alla data di presentazione del primo ricorso (05/02/2025), dunque, il cliente non aveva ancora evidenza che l'operazione sarebbe poi stata stornata. La richiamata circostanza esclude, dunque, che la presentazione del ricorso in esame costituisca una ipotesi di frazionamento indebito della domanda.
La materia, come noto, è regolata dal d. lgs. n. 11/2010 come modificato dal d. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- *Payment Services Directive 2*).

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *strong customer authentication* SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.
Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa *de qua* prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.
Risulta documentalmente che l'operazione contestata consiste in un pagamento eseguito il 13.12.2024, alle ore 16.59, per un ammontare di € 990,00.
Dai log informatici versati in atti, nonché dalla legenda esplicativa, emerge che essa sia stato effettuato un accesso all'area riservata dall'applicazione presente sul dispositivo del cliente, autorizzato mediante il "riconoscimento biometrico disponibile sullo smartphone per l'accesso". Il Collegio deve rilevare che detto accesso sia avvenuto in modalità conforme a SCA, risultando *per tabulas* la presenza di entrambi i fattori di autenticazione: il possesso dello smartphone autenticato (elemento di possesso) e il fattore biometrico (elemento di inerenza).
Di seguito, si evidenzia che alle ore 16:38 è stato eseguito un accesso da web con autenticazione forte, mediante l'inserimento di username e password (elemento di conoscenza) nonché inserimento di OTP ricevuto sul numero di cellulare univocamente associato al conto (elemento di possesso). Del resto, lo stesso cliente, in denuncia, indica che comunicava al truffatore il codice ricevuto via sms.
Su tale fase prodromica all'esecuzione dell'operazione appaiono convergenti le osservazioni di cui alla decisione n. 257315/2025, resa da questo Collegio.
Successivamente, si registra alle ore 16:39 la consultazione del PIN della carta di debito, in modalità conforme a SCA, poiché avvenuto mediante riconoscimento biometrico e conferma dell'operazione tramite token.
Immediatamente dopo, alle ore 16:40 veniva registrata una procedura di cambio di tale password, eseguita da web.
L'intermediario sottolinea che questa procedura di cambio password rappresenta un nuovo accesso con autenticazione forte, propedeutico alla corretta esecuzione dell'operazione di pagamento contestata; parte resistente osserva, al riguardo, che la password di accesso all'area riservata può essere modificata sia tramite app sia tramite web tramite inserimento di username, due delle quattro cifre del PIN della carta di debito e dell'OTP ricevuto tramite sms.
Nel caso di specie, le tracciature informatiche evidenziano che la modifica sia avvenuta mediante all'inserimento di username, di due cifre del PIN, nonché di apposito codice OTP ricevuto tramite sms al numero di cellulare univocamente associato al conto del cliente.
Come pure accertato da questo Collegio "Nella fase di cambio password, i fattori di autenticazione sono il codice PIN e le credenziali statiche (elemento di conoscenza) e il codice monouso OTP inviato tramite SMS sullo smartphone del cliente (elemento di possesso)" (cfr. dec. n. 257315/2025).
La fase precedente all'esecuzione del pagamento contestato si è conclusa con la modifica dei massimali della carta di debito, alle ore 16:58:40, avvenuta mediante autenticazione forte con

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

inserimento di username e password (elemento di conoscenza) e inserimento di codice OTP ricevuto con SMS sul numero di cellulare univocamente associato al conto corrente (elemento di possesso).
Quanto al pagamento, dalla lettura dei log informatici risulta che siano stati inseriti l'username e la password personali, a cui ha fatto seguito la digitazione del codice OTP inviato tramite sms al dispositivo autenticato del cliente, contenente l'avvertimento che sarebbe stato necessario digitare detto codice per la generazione del CVV della carta.
La generazione del CVV dinamico risulterebbe quindi avvenuta mediante l'inserimento delle credenziali (elemento di conoscenza) e il possesso del dispositivo mobile autenticato (elemento di possesso).
Alle ore 16:59 risulta disposto ed eseguito il pagamento di € 990,00, che – secondo la prospettazione dell'odierno resistente – risulterebbe eseguito con autenticazione forte attraverso inserimento (oltre che delle credenziali statiche dalla carta) del CVV dinamico, nonché con inserimento di OTP ricevuto tramite SMS.
Tuttavia, alla luce delle evidenze in atti, se il codice OTP sms rappresenta – ai fini dell'autenticazione dell'operazione disconosciuta – il fattore di possesso, si pone il problema di individuare il secondo fattore di autenticazione. In particolare, è necessario stabilire la valenza attribuibile al codice CVV dinamico, che l'intermediario qualifica come elemento di "conoscenza".
Non può sottacersi, infatti, che – alla luce delle indicazioni fornite dall'EBA nell'Opinion del 21 giugno 2019 – il CVV dinamico debba essere definito come elemento di possesso; l'orientamento condiviso dei Collegi appare conforme a tali indicazioni, così come pure la decisione di questo Collegio in merito alla medesima fattispecie (cfr. dec. n. 257315/2025 cit.).
Ne deriva, pertanto, che un doppio fattore di possesso non risulta conforme alla SCA in quanto, in base alla citata Opinion dell'EBA, l'autenticazione forte presuppone il ricorso a due fattori di autenticazione appartenenti a categorie diverse.
La mancanza anche parziale della prova del rispetto dei presidi di sicurezza in tutte le fasi dell'operazione di pagamento, e quindi sin da quella di accesso al sistema, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente, costituendo, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente (cfr. Coll. coord., dec. n. 22745/2019).
Deve, pertanto essere riconosciuto il diritto del ricorrente ad ottenere il rimborso del controvalore dell'operazione contestata.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 990,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA