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) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 01/07/2025

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 19/03/2024, una telefonata – preannunciata da un SMS inserito nella chat genuina dell'intermediario – nel corso della quale un sedicente operatore dell'istituto la informava di azioni sospette sulla sua carta di debito (a causa dell'identità del beneficiario, nonché del superamento dei massimali), per via delle quali si rendevano necessari verifiche e movimenti di prova.
Faceva presente che l'interlocutore le avesse chiesto conferma del suo nome utente, la conferma di solo 2 caratteri della sua password e del suo indirizzo e-mail e le avesse fatto autorizzare una transazione di € 2.900,00, celata dalle suddette presunte verifiche; sottolineava che i messaggi contenenti i codici di autorizzazione non riportassero mai il motivo della richiesta, e dunque non fosse possibile identificare uno scopo fraudolento.
Soggiungeva che, terminata la telefonata, avesse chiamato il servizio clienti dell'intermediario una prima volta per sincerarsi della correttezza dell'operazione (venendo a sapere di essere stata truffata) ed una seconda volta per resettare i propri accessi (risultando bloccata l'app); solo in tale ultima occasione le veniva consigliato di sporgere denuncia e di produrne evidenza.

Affermava che, in seguito, avesse nuovamente contattato l'intermediario per verificare lo stato dell'operazione e fosse venuta a conoscenza del fatto che la propria carta di debito fosse stata distrutta e ne fosse stata inviata una nuova, senza che le fosse stato notificato alcunché.
In seguito alla contabilizzazione e al conseguente addebito dell'importo della transazione, deduceva di aver disconosciuto l'operazione e di aver presentato reclamo all'intermediario, chiedendo come fosse stato possibile tutto ciò, trattandosi di un'operazione il cui controvalore superava i massimali consentiti.
Non avendo ottenuto positivo riscontro, chiedeva il rimborso della somma di € 2.900,00.
Costituitosi ritualmente, l'intermediario rilevava che la cliente fosse stata ragionevolmente vittima di vishing; ciò nonostante riteneva che la sua condotta fosse connotata da colpa grave per avere dato seguito ad una telefonata truffaldina e per avere condiviso tutti i codici OTP ricevuti sul proprio numero di cellulare, come dalla stessa ammesso in denuncia, necessari per modificare la password, accedere all'home banking, generare i due CVV dinamici, associare la carta ad un wallet ed eseguire il pagamento contestato.
Precisava che la ricorrente non avesse fornito alcuna prova circa la riconducibilità alla banca del numero da cui era stata contattata e che la truffa occorsa non potesse ritenersi particolarmente sofisticata, poiché esiste in commercio una banale tecnica che permette ai truffatori di inviare SMS ed effettuare telefonate facendo visualizzare al destinatario un nome e un numero prescelti in luogo di quelli reali.
Riteneva che ciò non potesse esserle in alcun modo imputabile, avendo adeguatamente informato la propria clientela a riguardo.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale ribadiva di non aver ricevuto alcuna risposta alla richiesta, inviata via pec, di ottenere informazioni circa i movimenti di accredito e addebito non giustificati.
Evidenziava che l'iniziale accredito della somma contestata ed il successivo riaddebito fossero sono entrambi avvenuti nella stessa giornata, senza intervalli di verifica tra i due momenti e che l'accesso al conto corrente fosse stato bloccato, nonostante non si fosse verificata alcuna operatività, se non quella perpetrata arbitrariamente dall'intermediario senza autorizzazione.
Sottolineava che l'indicazione, ricevuta dall'intermediario, di attendere la contabilizzazione dell'operazione contestata prima di poter procedere al disconoscimento non fosse coerente con i log allegati.
Contestava che la truffa potesse considerarsi poco sofisticata, anche perché la e-mail riportante le modalità di contatto da parte del servizio clienti era stata inviata ai correntisti soltanto in data successiva rispetto alla truffa.
Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale reiterava quanto già spiegato nelle controdeduzioni, ripetendo che se il sedicente operatore aveva già l'accesso al profilo della cliente oppure conosceva i suoi dati sensibili, la colpa di quest'ultima era ancora più evidente, poiché aveva permesso a terzi di accedere al proprio conto corrente, fornendo dati bancari privati.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione, successivamente disconosciuta.
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*).
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 on line eseguito il 19/3/2024 alle ore 17:39, per un importo di € 2.900,00.
In sede di denuncia la cliente ammette di avere fornito al sedicente operatore dell'intermediario sette codici OTP, che – secondo l'intermediario – sarebbe stati utilizzati per accedere all'home banking; modificare la password; modificare i massimali della carta di debito; generare due CVV dinamici; associare la carta ad un wallet (il quale però non è poi stato utilizzato) ed eseguire il pagamento contestato.
Al riguardo, mentre dall'esame delle dichiarazioni della ricorrente sembrerebbe che la stessa si sia limitata a fornire i codici OTP ricevuti, dunque senza intervenire direttamente nell'esecuzione dell'operazione contestata, le allegazioni presenti nel ricorso farebbero supporre una collaborazione della stessa durante la fase autorizzativa della transazione.
Con riferimento a fattispecie analoghe l'orientamento uniforme dei Collegi ha chiarito che se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non deve intendersi, per ciò solo, 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 prestatore dei servizi di pagamento.
Laddove, invece, l'operazione di pagamento on-line sia stata preparata dal truffatore che ha a disposizione i codici dispositivi del cliente, questa non può ritenersi eseguita per intero dal pagatore, e quindi non può considerarsi sussistente il requisito necessario per escludere il regime di responsabilità previsto dalla PSD2. Nel caso di specie, dunque, può escludersi che l'operazione possa considerarsi eseguita personalmente dalla ricorrente.
Dai log informatici versati in atti emerge che l'accesso alla home banking sia avvenuto per il tramite del cellulare univocamente associato al conto corrente della cliente, la quale è stata registrata con riconoscimento biometrico; pertanto, risulta che esso sia avvenuto mediante il solo fattore di inerenza costituito dal riconoscimento biometrico, poiché le tracciature informatiche non rilevano la registrazione del secondo fattore di autenticazione.
Al riguardo, l'intermediario ha precisato che esso sia avvenuto senza la necessità dell'inserimento di un secondo fattore di autenticazione, ai sensi dell'art. 10 del Regolamento Delegato (UE) 2018/389, che autorizza i PSP a non applicare la SCA qualora non siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha effettuato un accesso con doppio fattore.
La norma appena richiamata, come modificata dal Regolamento Delegato (UE) 2022/2360, consente invero che l'accesso c.d. informativo al conto possa avvenire senza applicare la SCA, a condizione che non siano decorsi più di 180 giorni dall'ultima applicazione della SCA.
Rispetto alla richiamata disposizione normativa, si pone la questione di stabilire se, una volta avuto accesso al conto mediante ricorso a un unico fattore (in applicazione della citata esenzione dalla SCA), sia o meno possibile riutilizzare detto fattore e combinarlo con un secondo elemento di autenticazione per autorizzare un'operazione di pagamento.
Sul tema si è pronunciata l'EBA (cfr. Q&A 2018_4141) la quale ha chiarito che il Regolamento delegato consente di riutilizzare uno dei fattori di autenticazione inseriti per l'accesso al conto per disporre un'operazione di pagamento online nell'ambito della medesima sessione, purché l'associazione di entrambi fattori produca il *dynamic linking* richiesto dall'art. 5 del Regolamento stesso; l'Autorità ha pure precisato (cfr. Q&A 2020_5516) che tale principio trova applicazione anche allorché l'accesso al conto non sia presidiato da SCA, in quanto riconducibile a una delle ipotesi per le quali è prevista l'esenzione ai sensi dell'art. 10 del Regolamento delegato. In tali casi, è possibile per gli intermediari riutilizzare l'(unico) elemento utilizzato per l'accesso al conto ai sensi dell'esenzione di cui all'art. 10, quando è eseguita un'operazione di pagamento elettronico nell'ambito della stessa sessione, a condizione che siano soddisfatte le condizioni appena descritte.
Nel caso di specie, a prescindere da quanto dedotto dall'intermediario il Collegio rileva – come già ha avuto occasione di chiarire in altri precedenti – che l'accesso non ha preceduto un'operazione meramente informativa, bensì un cambio di password, necessario poi per effettuare l'operazione dispositiva vera e propria; esso, quindi, non può ritenersi rientrante nell'ambito di applicazione del richiamato art. 10, con la conseguenza che non può considerarsi applicabile la prevista esenzione dalla SCA (cfr. Coll. Milano, dec. n. 10636/2024; n. 8155/2024; n. 7574/2024).

In considerazione del fatto che le stesse indicazioni dell'EBA precisano che – laddove il cliente disconosca le operazioni eseguite in applicazione di una esenzione dalla SCA normativamente prevista – resta comunque ferma la responsabilità dell'intermediario che ha deciso di non adottare l'autenticazione forte, fatte salve le ipotesi di frode dell'utilizzatore.
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 € 2.900,00.
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