COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore PIERFRANCESCO BARTOLOMUCCI

Seduta del 09/01/2025

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che in data 02/02/2024, alle ore 18:19, avesse ricevuto una telefonata nel corso della quale l'interlocutore, qualificatosi come operatore del servizio antifrode della banca, le comunicava che fossero in atto delle operazioni sospette e verosimilmente fraudolente sul suo conto, relative all'acquisto di criptovalute, attraverso due prelievi dal suo conto per gli importi di € 10.000,00 ed € 3.000,00.
Faceva presente di aver controllato sul sito istituzionale della banca che il numero di telefono di provenienza della chiamata corrispondesse effettivamente a quello del proprio istituto e che, nel corso della telefonata, il sedicente operatore avesse dimostrato di essere in possesso di rilevanti dati personali, insistendo affinché quest'ultima comunicasse i codici a lei pervenuti tramite SMS, al fine di bloccare le disposizioni effettuate per l'acquisto di criptovalute.
Sottolineava, essendosi persuasa dell'urgenza di sventare un'operazione fraudolenta ai suoi danni, di aver comunicato all'operatore i numeri generati dalla banca e trasmessi via SMS, ma che, insospettita, avesse contattato in seguito il numero verde dell'intermediario, avvedendosi così di essere caduta vittima di una truffa e in particolare di aver autorizzato un bonifico ordinario dell'importo di € 9.999,00.

Osservava di aver insistito nel chiedere, alla vera operatrice della banca, di sospendere ed annullare immediatamente l'ordine di bonifico, ricevendo conferme in tal senso, salvo apprendere, svariate ore più tardi, che l'operazione si fosse già perfezionata.
Quanto all'operazione disconosciuta precisava che il bonifico ordinario operato dai truffatori fosse stato effettuato di venerdì, alle ore 19:10 e che lei avesse chiesto alle ore 19:30 alla vera operatrice della banca di revocare immediatamente detto bonifico, essendo in atto una truffa.
Deduceva di aver sporto denuncia alle competenti Autorità e di aver inutilmente presentato reclamo all'intermediario.
Riteneva che non sussistesse l'elemento della colpa grave a proprio carico poiché, malgrado le modalità particolarmente insidiose adottate dai truffatori, si era adoperata con diligenza più che ordinaria per assicurarsi che il numero da cui la telefonata fosse pervenuta fosse effettivamente quello indicato dalla banca; al contrario, contestava che l'intermediario avesse omesso di identificare il beneficiario della disposizione e di rilevare che si trattasse in realtà di un frodatore e che non avesse bloccato tempestivamente l'operazione, nonostante avesse ricevuto il relativo ordine solo dopo venti minuti dall'esecuzione del bonifico fraudolento.
Chiedeva, pertanto, il rimborso delle somme illecitamente sottratte.

Costituitosi ritualmente, l'intermediario rilevava che l'operazione di bonifico contestata fosse stata correttamente contabilizzata, registrata e autenticata, in quanto posta in essere con il corretto inserimento delle credenziali.
Riteneva che sussistesse la colpa grave della cliente, la quale, con il proprio negligente comportamento, aveva permesso la realizzazione della truffa in cui era caduta vittima; aveva vanificato e ignorato tutte le misure di protezione poste in essere dalla banca; aveva dato seguito alle richieste di un sedicente operatore al telefono ed aveva comunicato tutte le OTP ricevute per eseguire le operazioni oggi disconosciute.
Precisava che il numero di telefono dal quale era pervenuta la chiamata fosse un numero verde e dunque legittimato solo a ricevere chiamate e non ad effettuarle; rilevava, altresì, che con l'impiego di una media diligenza, la cliente avrebbe dovuto certamente dubitare e porre fine alla telefonata, tenuto conto del carattere d'urgenza che, come ormai noto a tutti, caratterizza gli attacchi di *phishing*.
Contestava la doglianza relativa alla mancata identificazione del beneficiario, precisando che la banca identifica correttamente tutti i propri clienti in conformità alle norme di legge; faceva altresì presente di diffondere apposite campagne informative volte a sensibilizzare la clientela rispetto alle forme più comuni di frode informatica.
Quanto al bonifico oggetto di disconoscimento, osservava che al momento della richiesta da parte della ricorrente, non potesse più essere annullato in quanto già lavorato dalla banca e trasferito sul conto corrente beneficiario, sempre aperto presso la banca medesima. Infatti, l'Accordo quadro sottoscritto, all'art. 38, Sezione I (cfr. All.1), prevede espressamente che solo gli ordini di pagamento ricevuti dopo le ore 21:00 di un giorno lavorativo saranno considerati ricevuti il giorno lavorativo successivo. Nel caso di specie, il bonifico era stato eseguito alle ore 19:00 quindi lavorato immediatamente dalla banca.
Segnalava, comunque, di aver provveduto al blocco cautelativo dell'operatività del conto corrente beneficiario del pagamento a seguito del ricevimento della chiamata da parte della ricorrente, in data 02/02/2024, ma che – ciò nonostante – parte delle somme fossero già state disposte dal titolare del conto.
Rilevava pure che, grazie alla tempestività del blocco, avesse vincolato sul conto corrente l'importo di € 5.027,90, restituito alla cliente in data 18/04/2024 ad esito delle apposite procedure di verifica interna.

Chiedeva, pertanto, in via principale il rigetto del ricorso e, in via subordinata, in caso di accertamento della propria responsabilità e ravvisata la colpa grave della ricorrente, di riconoscere il concorso di colpa nella misura del 50% dell'importo non ancora restituito.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale ribadiva che non fosse riscontrabile a proprio carico alcun comportamento fraudolento, ovvero affetto da dolo o colpa grave; riteneva, invece, sussistente la responsabilità della banca anche a causa del tardivo intervento di blocco del conto destinatario del bonifico e della conseguente solo parziale restituzione, avvenuta a distanza di oltre due mesi dal disconoscimento.
Riteneva che la circostanza secondo cui la telefonata fosse pervenuta da un numero verde non potesse essere considerata come indice di colpa grave della vittima della truffa; deduceva, inoltre, che l'intermediario non avesse nemmeno fornito prova, né indicato il fattore di autenticazione, relativo all'iniziale operazione di cambio password, e che non avesse neppure dato evidenza della comunicazione dei dati da parte della ricorrente al falso operatore.
Chiedeva, pertanto, il riconoscimento del proprio diritto ad ottenere il controvalore del bonifico fraudolento, al netto di quanto già restituito, per il corrispondente importo di € 4.971,10, oltre interessi "computati secondo i termini previsti dalla linea di deposito aperta".

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale sottolineava – quanto al numero verde – che fosse ormai fatto notorio nonché orientamento costante dell'ABF, che i "Numero Verde" siano abilitati solo a ricevere e non ad effettuare le chiamate; specificava, inoltre, che esiste comunemente in commercio una banale tecnica che permette ai truffatori di effettuare telefonate facendo visualizzare al destinatario un nome e numero prescelto in luogo del vero numero del mittente.
Al riguardo, riteneva che ciò non potesse essere in nessun modo imputabile alla banca, la quale non può evitare e/o bloccare tale tipologia di telefonate/SMS, ma mette in guardia i clienti con apposite informative.
Ribadiva poi che la cliente avesse dato seguito alla telefonata con il sedicente operatore ed avesse ammesso, in sede di denuncia, di aver fornito il proprio codice fiscale e di aver comunicato i codici OTP ricevuti, nonostante il contenuto degli SMS fosse chiaro in merito alle finalità delle OTP condivise.
Richiamava pure la tempestività del blocco adoperato sul conto corrente del beneficiario a seguito della segnalazione della cliente, nonché l'avvenuta restituzione dell'importo di € 5.027,90 alla cliente in data 18/04/2024.

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 (cosiddetta 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 (cosiddetta *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 bonifico eseguito il 02/02/2024 alle ore 19:00 per un ammontare di € 9.999,00.
Mette conto rilevare che risulta pacifico e incontestato tra le parti il fatto che l'intermediario abbia provveduto a rimborsare al cliente la somma di € 5.027,90, ancora disponibile sul conto corrente del beneficiario del bonifico contestato, tanto che la stessa ricorrente ha ridotto il *petitum* al minor importo di € 4.971,10.

Ciò premesso, parte resistente dichiara che il primo accesso all'area riservata sia stato registrato alle ore 18:27:30 del 02/02/2024, con richiesta di reset della *password*. Descrive quindi il procedimento di recupero, sottolineandone la conformità alla SCA; esso può avvenire, utilizzando l'app o il web, mediante i seguenti passaggi: 1. inserimento della username scelta dal cliente in sede di apertura del rapporto (questa username, inoltre, può essere recuperata attraverso la funzione "Hai dimenticato il tuo nome utente?" inserendo il codice fiscale del cliente); 2. inserimento di due delle quattro cifre del PIN della carta di debito associata al Conto Corrente (fattore di conoscenza), prese randomicamente dal sistema; 3. inserimento di una OTP ricevuta tramite SMS (fattore di possesso) sul numero di cellulare indicato dal cliente in sede di apertura del rapporto e univocamente associato al conto.
Nel caso di specie, l'intermediario afferma che la procedura di reset della password sia stata correttamente completata grazie all'inserimento di username e di due cifre del PIN, conosciute solo dalla ricorrente (primo fattore: fattore di conoscenza) oltre che di un apposito codice OTP (secondo fattore: fattore di possesso) ricevuto tramite SMS al numero di cellulare univocamente associato al conto della ricorrente; precisa pure che la ricorrente, prima di tale operazione, abbia ricevuto anche un codice OTP con l'indicazione dell'username associato alla sua utenza, che avrebbe presumibilmente fornito al sedicente operatore per permettere l'avvio della procedura di cambio *password*.
Dalle tracciature informatiche e dalla rispettiva legenda esplicativa versate in atti emerge, effettivamente, che l'operazione di reset password (codice 171 – "Inserimento di username, due cifre del PIN della carta di debito e OTP inviata via SMS") sia stata autorizzata mediante il ricorso a un elemento di conoscenza (due cifre del PIN – oltre alla *username* che però non rileverebbe come elemento di conoscenza ai sensi degli orientamenti EBA) e a un elemento di possesso (l'OTP SMS inviata alla cliente).
Secondo la ricostruzione di parte resistente, a tale primo cambio di *password* ha fatto seguito un ulteriore tentativo di modifica, ma da un indirizzo IP diverso da quello

usualmente utilizzato dalla cliente; ciò avrebbe determinato – secondo le regole antifrode della banca – il blocco automatico ("bloqueo Soft") all'accesso all'area riservata della ricorrente, che è stata superata solo grazie ad un ulteriore tentativo di cambio, secondo la procedura ordinaria appena descritta.
Anche di tali ulteriori circostanze v'è riscontro documentale nei log prodotti in atti.
Quanto alla fase di accesso all'area riservata, prodromica alla esecuzione del bonifico, l'intermediario rileva che alle ore 19:00 esso sia avvenuto tramite inserimento di *username* e *password*; i log versati in atti confermano la riferita circostanza ("Medio de autentificaciòn: autenticaciòn con usuario y password personales").
L'intermediario precisa altresì che detto accesso all'area riservata della ricorrente sia avvenuto senza la necessità dell'inserimento di un secondo fattore di autenticazione, ai sensi dell'art. 10 del Regolamento Delegato (UE) 2018/389, "poiché solo pochi minuti prima era stato eseguito l'accesso con doppio fattore mediante modifica della password".
La norma appena richiamata, come modificata dal Regolamento Delegato (UE) 2022/2360, consente invero che l'accesso cosiddetto 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, il Collegio rileva – come già ha avuto occasione di chiarire in altri precedenti – che l'accesso al conto non sia stato di carattere meramente informativo, bensì di tipo operativo, essendo stato effettuato per finalizzare l'operazione di bonifico; pertanto, questo 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, il ricorso deve essere accolto.
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 infatti 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 della ricorrente ad ottenere il rimborso del controvalore dell'operazione contestata, al netto dell'importo che ha già formato oggetto di ripetizione da parte dell'intermediario.
Attesa la natura restitutoria dell'obbligazione di rimborso, devono altresì essere riconosciuti gli interessi al tasso legale, da liquidarsi nel rispetto della norma di cui all'art. 11 del D.lgs. n. 11/2010; l'importo di € 4.971,00, pertanto, deve essere rimborsato con giusta valuta.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.971,00, con buona valuta.
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