COLLEGIO DI MILANO

composto dai signori:

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

Relatore PIERFRANCESCO BARTOLOMUCCI

Seduta del 17/12/2024

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che in data 11.05.2024 fosse stato contattato telefonicamente da un sedicente operatore dell'intermediario, che gli chiedeva se avesse disposto bonifici per l'acquisto di criptovalute; precisava che la chiamata provenisse dal numero di telefono riconducibile alla banca.
Soggiungeva che l'operatore lo avesse invitato a bloccare urgentemente il pagamento seguendo le sue istruzioni, ricevute tramite il canale SMS abitualmente utilizzato dall'intermediario; l'interlocutore dimostrava di conoscere correttamente i dati personali del cliente, rendendosi in tal modo credibile.
Seguiva pertanto le indicazioni, con conseguente esecuzione di un pagamento truffaldino di € 2.980,00.
Riteneva sussistente la responsabilità dell'intermediario per aver consentito la violazione dei propri dati personali da parte di terzi, che avevano avuto la possibilità di contattarlo costringendolo a prendere una decisione in un ristretto lasso temporale.
Chiedeva, pertanto, il rimborso del controvalore dell'operazione disconosciuta.
Costituitosi ritualmente, l'intermediario rilevava che l'operazione fosse stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali.

Considerava sussistente la colpa grave del cliente, il quale, con l'impiego di una media diligenza, avrebbe dovuto dubitare delle richieste dell'operatore e, leggendo con attenzione il testo degli SMS con le OTP, avrebbe certamente dovuto accorgersi che stava autorizzando un pagamento, piuttosto che fornire i codici riservati necessari per l'esecuzione dell'operazione.
Osservava, peraltro, di aver diffuso apposite campagne informative volte a sensibilizzare la clientela rispetto alle forme più diffuse di frode.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale precisava che la truffa fosse del tutto credibile in quanto generata da una telefonata riconducibile all'intermediario; peraltro sottolineava il fatto che il truffatore fosse in possesso dei suoi dati privati, rendendo evidente l'inidoneità dei sistemi di sicurezza dell'intermediario.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale evidenziava che esistono strumenti che consentono al truffatore di effettuare telefonate facendo visualizzare al destinatario un nome e numero prescelto in luogo del vero numero del mittente.
Ribadiva che non vi fosse stato alcun malfunzionamento o compromissione dei sistemi di sicurezza di della banca, pertanto – con l'impiego di normale diligenza – il cliente avrebbe potuto accorgersi dell'anomala telefonata, nonché delle strane richieste del sedicente operatore, ma soprattutto prestare attenzione agli SMS ricevuti, che spiegavano precisamente le finalità delle OTP che, con colpa grave, aveva fornito al truffatore.

DIRITTO

La domanda proposta dal 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 bonifico eseguito il 11.5.2024 alle ore 16:37 per un ammontare di 2.980,00 €.
Tanto premesso, parte resistente dichiara che siano stati eseguiti due accessi all'area riservata, cui è seguita la modifica dei massimali della carta; in particolare, un primo accesso alle ore 16:14:15 (log accessi riga 77) mediante riconoscimento biometrico [Medio de autentificación (colonna E) = "106"] ed un secondo, effettuato pochi minuti dopo, alle 16:21:39 (log accessi riga 76), eseguito accesso con username e password [Medio de autentificación (colonna E) = "02"].
Dalle tracciature informatiche versate in atti e della relativa legenda, risulta che effettivamente detti accessi, registrati il giorno della frode (11/05/2024), siano stati autorizzati mediante il ricorso – rispettivamente – a un elemento di inerenza (la biometria) e a un elemento di conoscenza (la password). Allo stesso tempo, emerge pure che essi siano stati eseguiti senza l'utilizzo del secondo fatto di autenticazione.
A tale specifico riguardo, l'intermediario richiama l'art. 10 del Regolamento delegato (UE) 2018/389, come modificato dal Regolamento Delegato (UE) 2022/2360, il quale consente 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) 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 la modifica dei limiti operativi e dispositivi dello strumento di pagamento; pertanto, questa 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; giova rilevare, inoltre, che l'intermediario non abbia neppure fornito alcuna prova circa l'operazione asseritamente avvenuta nel termine dei 180 giorni precedenti.
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; essa

rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.
Deve, pertanto essere riconosciuto il diritto della 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 € 2.980,00.
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