

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) DALMARTELLO | Membro di designazione rappresentativa degli intermediari |
| (MI) CESARE | Membro di designazione rappresentativa dei clienti |

Relatore (MI) CESARE

Seduta del 11/03/2025

FATTO

Il cliente afferma che in data 27/03/2024 riceveva un sms apparentemente proveniente dall'intermediario convenuto con il quale le veniva comunicata l'attivazione di un token. L'operatore la invitava a contattare il numero telefonico ivi riportato qualora non avesse riconosciuto l'operazione descritta. Contattato il numero indicato, riferisce di aver parlato con un sedicente operatore, che peraltro già in possesso dei suoi dati personali. In data 15/04/2024 il ricorrente afferma di aver ricevuto ulteriori chiamate dal medesimo operatore, che la invitava a disinstallare l'app di *homebanking* per completare la certificazione del dispositivo e dell'identità. In data 19/04/2024, controllato il conto corrente, ha poi appreso dell'esecuzione di 18 operazioni fraudolente per un valore complessivo di euro 17.264,00. le operazioni presentavano evidenti anomalie di tempistiche, importi e beneficiari, mai conosciuti dalla cliente. In data 22/04/2024 l'intermediario ha riconosciuto la frode, ma non ha ammesso alcuna responsabilità, offrendo un rimborso parziale di euro 8.263,00. Il 15/07/2024 il ricorrente presentava formale reclamo, senza esito. Il cliente quindi, chiede che la banca sia tenuta alla consegna della documentazione anche informatica richiesta con il reclamo del 15/07/2024 e inoltre, che venga accertata la responsabilità contrattuale ed extracontrattuale – anche ex art. 2050 c.c. e per la violazione della normativa sul trattamento dei dati personali,

nonché il rimborso di € 17.264,00, oltre ad interessi e rivalutazione dalla data delle operazioni fino all'effettivo rimborso nonché di ogni altro onere collegato.

Nelle controdeduzioni, l'intermediario afferma l'inammissibilità del ricorso per i profili attinenti alla privacy poiché estranea alla competenza dell'ABF; inoltre, rileva come il messaggio civetta non sia in alcun modo riferibile al numero ufficiale della banca. Peraltro, eccepisce che i bonifici disconosciuti sono stati inseriti ed autorizzati con le credenziali di sicurezza della ricorrente, con una operatività che evidenzia l'invio dei codici all'operatore da parte del cliente: la ricorrente ha pertanto permesso l'attivazione del secondo codice di verifica che ha consentito l'attivazione del secondo mobile token in mano ai malfattori, dopo aver disinstallato peraltro l'app seguendo le istruzioni di quest'ultimo. Simile contegno viola i doveri di custodia e protezione delle credenziali di sicurezza e qualifica come grave la colpa del cliente, esonerando l'intermediario da ogni addebito.

La banca rinnova la propria disponibilità al rimborso parziale per € 8.263,00, previa sottoscrizione di malleva a mani del cliente, ma senza riconoscimento di responsabilità.

Le operazioni disconosciute sono del resto debitamente contabilizzate e autorizzate e non presentano alcuna anomalia

Per queste ragioni, l'intermediario chiede che questo ricorso venga respinto poiché infondato.

DIRITTO

La controversia sottoposta all'esame del Collegio verde sul rimborso di somme indebitamente sottratte a seguito di diciotto disposizioni fraudolentemente impartite per complessivi € 17.264,00.

Le operazioni contestate rientrano nell'ambito di applicazione della disciplina del D. Lgs. 27/1/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).

La normativa richiamata ha ripartito diversi obblighi tra il prestatore di servizi di pagamento e l'utilizzatore. Quest'ultimo, in particolare, ha il dovere di adoperare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici PIN). Per quanto riguarda l'intermediario, la normativa ricordata prevede l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi. Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.

La normativa mostra un chiaro favore nei confronti dell'utilizzatore: infatti, l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo oppure che questi abbia agito in modo fraudolento ovvero con dolo o colpa grave.

Alla luce di tali disposizioni, pertanto, due sono i passaggi da verificare.

In primo luogo è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova di per sé insufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore.

In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.

Con riferimento alla *strong customer authentication* (c.d. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 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). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerzia; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Dalle evidenze prodotte dall'intermediario per l'accesso prodromico alle operazioni contestate risulta che è stato effettuato un accesso riconducibile all'id utente della cliente con il dispositivo su cui era stato in precedenza attivato il nuovo mobile token.

Risulta evidenza dell'OTP (fattore di possesso) ma non si riscontra l'inserimento del PIN, il cui utilizzo risulta solo dalla descrizione "attività", mentre la colonna "esito operazione" nel log prodotto non è valorizzata.

E' stato poi prodotto il log di un successivo accesso da un dispositivo diverso da quello registrato; nei log prodotti non risulta valorizzato l'inserimento del PIN e l'esito dell'operazione; vi è poi evidenza di un invio dell'OTP via mail (e non via SMS come riferito dall'intermediario) senza l'indicazione però dell'indirizzo di posta del destinatario.

Poiché il primo token e l'operazione successiva che ha autorizzato un nuovo *device* risultano prive del PIN, non vi è prova nemmeno dell'esito delle successive operazioni contestate: pertanto la SCA non può ritenersi provata (cfr. Collegio di Milano 4760/2024). Consegue che non possono ritenersi dimostrate nemmeno le operazioni dispositivo, effettuate in seguito all'autorizzazione ad operare con il nuovo dispositivo.

Ne consegue l'accoglimento parziale del ricorso, poiché è dovuta la restituzione del capitale oggetto delle operazioni fraudolente, ma non è dovuta la rivalutazione e gli interessi devono essere corrisposti con decorrenza dalla data del reclamo.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 17.264,00 oltre interessi legali dal reclamo al saldo.

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