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) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

PIERFRANCESCO BARTOLOMUCCI

03/12/2024

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che in data 06.02.2024, dopo che a sua insaputa ignoti avevano acquisito illecitamente le sue credenziali della *home banking*, avesse ricevuto un sms che sembrava provenire dall'intermediario, presso cui aveva aperto un conto corrente, con cui gli veniva comunicato che la banca avesse ricevuto dallo stesso un ordine di bonifico istantaneo on line di € 5.700,00 a favore di un conto corrente avente coordinate bancarie estere.
Precisava di aver contattato tempestivamente il numero verde messo a disposizione della banca al fine di disconoscere l'ordine di bonifico on line e di aver appreso che l'operazione di pagamento fosse già stata processata e di conseguenza il conto svuotato; soggiungeva di essersi recato personalmente presso la propria filiale per farsi assegnare le nuove credenziali, illecitamente sottratte, per l'utilizzo dell'*home banking* e di aver presentato denuncia-querela presso le Autorità.
Riteneva che l'istituto di credito non avesse minimamente tutelato il proprio cliente omettendo di impedire che utenti non autorizzati potessero entrare sul proprio conto corrente ed effettuare illecite operazioni di pagamento alla luce e lo considerava responsabile dell'accaduto, ai sensi dell'art. 1176, comma 2, cod. civ.

Chiedeva, pertanto, il rimborso dell'importo di € 5.700,00 e, in via subordinata, il risarcimento del danno e la rifusione delle spese di assistenza difensiva per € 1.500,00.

Si costituiva ritualmente l'intermediario, il quale eccepiva in via preliminare l'inammissibilità del ricorso, essendo state sollevate contestazioni aventi ad oggetto il tema della *privacy* ai sensi della disciplina del GDPR, che esulano dalla competenza dell'Arbitro.
Quanto al merito, deduceva che nel modulo del ricorso e nella denuncia allegata non venisse fatto riferimento ai dettagli e alle modalità di commissione della frode.
Sottolineava che il servizio "Rapporti a distanza tra Banca e Cliente" prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte", in linea con la normativa europea PSD2; soggiungeva di raccomandare da tempo la massima attenzione e cautela nell'utilizzo dei canali telematici, pubblicando avvisi specifici nella pagina di accesso al portale.
Faceva presente che le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; riteneva, quindi, che sussistesse la colpa grave del ricorrente per non avere adempiuto con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate del proprio strumento di pagamento. Sottolineava che il cliente non avesse nutrito alcun sospetto, neanche dopo aver ricevuto il messaggio di attivazione del (secondo) *Mobile Token* al suo cellulare, e successivamente, anche quello della certificazione del numero telefonico.
Rilevava, inoltre, l'incauto comportamento del ricorrente – connotato da colpa grave – per aver fornito e/o inserito le credenziali del proprio strumento di pagamento, consentendo a soggetti terzi l'attivazione del (secondo) *Mobile Token*.
Precisava, da ultimo, che non fossero stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.
Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale specificava di non aver mai ricevuto ed "abboccato" a nessuna telefonata e/o ad alcun messaggio da parte di terzi malintenzionati, né di aver cliccato alcun link malevolo e né, tantomeno, di aver smarrito né ceduto/divulgato a terzi le credenziali di sicurezza della propria *home banking*.
Ribadiva di non aver cooperato colposamente alla frode, avendo osservato tutti gli obblighi sussistenti in capo ad esso in qualità di utente dei servizi di pagamento, previsti dall' art. 7 del d. lgs. n. 11/2010.
Precisava di non aver ricevuto alcun sms di avvertimento (sms alert) da parte della banca, la quale – dal canto suo – non solo non aveva fornito la prova che l'operazione di pagamento fosse stata autenticata, correttamente registrata e non avesse subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione, ma non avesse nemmeno dato prova della condotta fraudolenta, dolosa o gravemente colposa tenuta dall'utente.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione on-line, successivamente disconosciuta.
In relazione ad essa, l'intermediario resistente ha spiegato un'eccezione preliminare di inammissibilità del ricorso, il cui *petitum* esorbiterebbe dalla competenza per materia

dell'Arbitro, in quanto avente ad oggetto questioni inerenti alla tutela del diritto alla riservatezza, disciplinata dal c.d. GDPR.
L'eccezione è infondata e non merita accoglimento.
Seppure il ricorrente abbia contestato nel reclamo la condotta dell'istituto di credito che non avrebbe impedito a terzi non autorizzati di accedere al proprio conto corrente ed effettuare illecite operazioni di pagamento, chiedendo il "rimborso di € 5.700,00 ai sensi dell'art. 7 e 10 comma 1 2 del D.lgs 11/2010 ed ai sensi dell'art. 82 del GDPR, oltre al risarcimento di tutti i danni subiti e subendi", nel ricorso questi chiede la ripetizione della somma di € 5.700,00 "fraudolentemente sottratta" (così implicitamente riferendosi alla disciplina dei servizi di pagamento), nonché – in via subordinata – il risarcimento dei danni subiti, senza richiamare in maniera espressa la disciplina sul trattamento dei dati personali.
Superata l'eccezione preliminare, nel merito mette conto rilevare che 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, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.
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.
Orbene, risulta *per tabulas* che l'operazione contestata consiste in un bonifico dell'importo di € 5.700,00 effettuato in data 06.02.2024, alle ore 11,31.
Con riferimento alla fase di attivazione del *mobile token*, l'intermediario ha precisato che avviene attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN, elementi di conoscenza) e del codice OTP inviato al cliente via SMS al cellulare collegato all'*home banking* (elemento di possesso); conformemente a ciò, in data 12/1/2024 alle ore 12:59 (molti giorni prima della asserita frode), ha dedotto di aver inviato al numero di cellulare del cliente il messaggio SMS e la notifica *push* relativi all'attivazione del secondo *mobile token* (il quale può essere attivato, solo mediante l'uso dei codici di sicurezza conosciuti solo dal cliente, fino a due *devices* diversi, e può sostituire il proprio telefono cellulare, cambiando modello, senza doverlo comunicare alla Banca).
Ciò premesso, dalle tracciature informatiche versate in atti emerge che in data 12/01/2024 alle ore 12:50 c'è stato un primo tentativo di accesso all'app con inserimento di ID utente e PIN, con visualizzazione dei *mobile token* attivi e invio via e-mail dell'OTP per l'attivazione

del *wallet*; nella stessa data, alle ore 12.58, c'è stato un secondo tentativo d'inserimento (campo "Attività: Tentativo di accesso con ID Utente e Pin"); il *mobile wallet* risulta attivato alle ore 13.00.
Seppure si rileva che l'ID utente fornito dall'intermediario corrisponde a quello che emerge nei log, non risulta invece l'inserimento del PIN, il cui utilizzo può essere desunto solo dalla descrizione attività utente; in relazione a ciò, l'odierno resistente sottolinea che l'attivazione è stata resa possibile dall'inserimento di un OTP ricevuto via sms, come si evince dal popolamento della corrispondente colonna della tracciatura informatica.
Risulta altresì *per tabulas* che l'attivazione del *mobile token* è successiva al tentativo di accesso all'app per il quale, al campo "Attività", risulta l'utilizzo di PIN+ID Utente (ancorché privo di OTP); inoltre, il numero a cui è stato inviato l'sms contenente l'OTP di attivazione coincide con il numero fornito dal cliente in sede di denuncia.
Con riguardo all'attivazione del nuovo *token*, pertanto, mentre risulta provato l'invio del codice OTP a un *device* in possesso del cliente (elemento di possesso), non può dirsi altrettanto con riguardo al secondo fattore (PIN), del cui inserimento non v'è piena prova.
Alle medesime conclusioni deve pervenirsi con riguardo alla procedura autorizzativa dell'operazione; emerge documentalmente che alle ore 11:28 del 06/02/2024 è stato eseguito l'accesso all'home banking con ID utente e Pin e generazione in app dell'OTP (come risulta dalla colonna OTP).
Al tempo stesso, però, risulta che prima e dopo l'accesso all'App e la disposizione del bonifico istantaneo risultano attività svolte tramite un *device* diverso da quello utilizzato per ordinare il bonifico contestato; emerge invece che l'IP del dispositivo con cui è stata effettuata l'operazione di pagamento non coincide con quello su cui è stato attivato il *mobile token* e non si ha diretta evidenza dell'inserimento del PIN. Inoltre non è neppure presente alcuna valorizzazione alla voce "esito operazione".
Da ultimo, quanto alla disposizione del bonifico contestato (avvenuta in data 06/02/2024 alle ore 11:31), l'intermediario afferma che l'operazione è stata autenticata tramite inserimento del PIN (elemento di conoscenza) e dell'OTP generato tramite *Token Wallet* (elemento di possesso); tuttavia, le risultanze documentali fanno emergere l'impiego del codice OTP (elemento di possesso), ma non anche del PIN che (come per la precedente fase di accesso) appare valorizzata solo nel campo attività.
Le stesse tracciature informatiche evidenziano che l'IP del *device* con cui è stato effettuato la disposizione non coincide con quello su cui è stato attivato il *Mobile Token*; inoltre, queste fanno pure emergere che – seppure il nome ed il modello del dispositivo utilizzato, il sistema operativo e la relativa versione sono uguali a quelli precedentemente analizzati – il numero di telefono non coincide con quello indicato nelle informazioni di base del cliente e nel modulo del ricorso, ma corrisponde a quello fornito all'atto di presentazione della denuncia.
Ancorché, nel caso di specie, si tratti di un'operazione autenticata nell'ambito della sessione precedentemente aperta, per la quale potrebbe ammettersi il "riutilizzo" di uno dei fattori di autenticazione precedentemente impiegati per l'apertura della sessione (secondo le linee guida dell'EBA), la mancata prova dell'uso del PIN impedisce di poter fare applicazione di tale principio nel caso di specie.
In relazione a quanto emerge dalla documentazione prodotta, deve quindi concludersi che il processo autorizzativo, nelle sue varie fasi, non risulti adeguato ai requisiti di autenticazione forte richiesti dalla normativa di settore, con la conseguenza che debba essere riconosciuto il diritto del ricorrente ad ottenere il rimborso della somma di € 5.700,00.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.700,00.
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