Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(BA) VITERBO	Membro designato dalla Banca d'Italia
(BA) COSTANTINO	Membro di designazione rappresentativa degli intermediari
(BA) ROBUSTELLA	Membro di designazione rappresentativa dei clienti

Relatore CARMELA ROBUSTELLA

Seduta del 29/11/2023

FATTO

Parte ricorrente, titolare di rapporti di conto corrente con l'intermediario A, riferisce che in data 29/11/2022 si recava presso la filiale dell'intermediario A per il ritiro della nuova carta associata al proprio conto ed in scadenza a gennaio 2023; in tale occasione gli veniva sottoposto un contratto con l'intermediario B, a cui era stato affidato il servizio di gestione delle carte.
Rappresenta di aver ricevuto la nuova carta presso la propria sede nel febbraio 2023 e rappresenta di aver effettuato il primo accesso sulla App in data 21/03/2023, attivando la funzione di SMS di avviso per le operazioni con importo superiore a € 50,00, di cui riceveva conferma dall'intermediario B tramite SMS.
Afferma che alle ore 11:51 del successivo 23/03/2023 riceveva sulla stessa utenza un SMS che lo informava circa la limitazione della carta/conto "per mancata verifica della sicurezza web".
Precisa che tale SMS si inseriva in coda ai messaggi genuini dell'intermediario B, era redatto in perfetto italiano e non presentava indici di anomalia. In considerazione di tali circostanze, afferma di aver cliccato sul link contenuto nel messaggio e di aver inserito nella pagina che si apriva i dati richiesti, relativi alla utenza associata alla carta dell'intermediario B. A tal punto, appariva sulla schermata del telefono la dicitura "Operazione non andata a buon

fine", seguita a distanza di pochi minuti da altro SMS che lo avvisava che sarebbe stato contattato a breve da un operatore.
Rappresenta di aver effettivamente ricevuto alle ore 13:10 una chiamata da una utenza telefonica riconducibile all'intermediario A, gli veniva comunicato di dover procedere alla verifica della sicurezza della carta per poter ottenerne la riattivazione. In particolare, il sedicente operatore enunciava alcuni dati di cui chiedeva conferma, quali codice fiscale e numero di cellulare; dopodiché richiedeva la conferma di tali dati tramite i codici OTP generati dal suo Token. Al termine di ogni operazioni riceveva Sms di conferma in coda ai precedenti messaggi autentici dell'intermediario B.
Riferisce, inoltre, di aver ricevuto alle ore 14:56 del 24/03/2023 una nuova chiamata sempre da una utenza associata all'intermediario A, con la quale un sedicente operatore lo invitava a generare ulteriori codici OTP. Lo stesso giorno alle ore 15:24 veniva contattato da un vero operatore dell'intermediario A, il quale lo allertava circa la disposizione di 6 bonifici dal suo conto, chiedendogli informazioni al riguardo. Afferma di non aver autorizzato i predetti bonifici e di aver ottenuto lo storno solo degli ultimi tre per un ammontare di € 118.970,00, restando invece addebbiatati sul conto i primi tre di importo pari ad € 148.950,00. Evidenzia che i codici OTP erano generati tramite Token one span codice e di non aver ricevuto alcuna notifica o richiesta di conferma delle operazioni, né una email di conferma di bonifici, come invece previsto dalla normativa vigente.
Provvedeva a sporgere querela in data 28/03/2023 e a presentare formale reclamo nei confronti di entrambi gli intermediari in data 05/04/2023, non ricevendo tuttavia l'accoglimento delle sue richieste.
Ritiene che i prelievi siano stati causati da un insufficiente sistema di protezione e vigilanza del conto Internet Banking da parte dell'intermediario A, oltre che alla difettosa protezione dei dati sensibili relativi alla carta di debito dell'intermediario B.
Fa presente che il truffatore era perfettamente a conoscenza di dati comunicati soltanto alla resistente B; lamenta la mancata attivazione del sistema di doppia autenticazione, nonché l'inerzia dell'intermediario A fronte di bonifici di rilevante entità, con causali contraddittorie e tra loro ravvicinati.
In particolare, evidenzia che le operazioni fraudolente sono state autorizzate da remoto con l'utilizzo di credenziali di un solo tipo (codici OTP). Sostiene, dunque, di essere stato vittima di una truffa insidiosa, realizzata attraverso SMS spoofing e Caller ID spoofing, tale da escludere la propria colpa grave o altro fatto impeditivo al risarcimento (richiama sul punto la normativa di riferimento e decisioni ABF) e chiede il rimborso delle somme indebitamente addebitate e disconosciute.
Costituitosi, l'intermediario A illustra preliminarmente: le modalità di accesso all'home banking tramite pc; le modalità di disposizione di un bonifico; le modalità di modifica dei dati personali a sistema.
Ritiene, dunque, che si tratti di un sistema di autenticazione basato su due fattori (uno di conoscenza e uno di possesso) e, dunque, conforme ai requisiti in materia di SCA previsti dalla direttiva PSD2.
Ciò premesso, ricostruisce la vicenda, rappresentando in particolare che alle ore 11:51 del 23/03/2023 il ricorrente ha ricevuto un sms nella stessa chat dell'intermediario B contenente un link truffaldino. Evidenzia come il ricorrente medesimo, cliccando sul link ricevuto, ha inserito le proprie credenziali di accesso, così comunicandole ai truffatori. Subito dopo ha ricevuto un secondo sms, in coda a quello precedente, dove gli è stata preannunciata la chiamata da parte di un operatore telefonico.
Successivamente, è stato contattato da un numero coincidente con quello di una delle sue filiali, in quanto i criminali avevano manipolato il numero telefonico del chiamante, realizzando un "call ID spoofing". Sottolinea che tale conversazione telefonica "è durata ben

34 minuti" e che i truffatori, ormai in possesso delle credenziali di accesso fornite dal ricorrente "dopo aver cliccato sul link fraudolento", si sono collegati via web browser alle ore 13:16, invitando il ricorrente a generare e poi a comunicare loro durante la telefonata un codice OTP. In particolare afferma che i truffatori alle ore 13:18 hanno modificato l'indirizzo email collegato al rapporto di Internet Banking, al fine di impedire che gli alert sull'esecuzione dei bonifici arrivassero al cliente. Fa presente che, ad ogni modo, il ricorrente ha ricevuto un alert relativo alla modifica dell'indirizzo mail associato al conto.
Alle successive 13:23 è stato registrato un nuovo accesso da dispositivo mobile e tra le ore 13:33 e 13:44 venivano autorizzati i tre bonifici fraudolenti. Rileva che le predette operazioni sono state effettuate dietro comunicazione dei codici OTP generati tramite il Token da parte del ricorrente, come da lui stesso affermato in denuncia. Rappresenta che il giorno successivo, tramite le stesse modalità, i truffatori hanno disposto tre ulteriori bonifici, i quali sono stati bloccati attraverso il recall in quanto non ancora partiti. Tutto ciò narrato, sostiene che le operazioni disconosciute siano state correttamente autenticate, registrate e contabilizzate, senza alcuna anomalia, non risultando peraltro superati i limiti operativi di importo previsti dal servizio, come confermato dai log informatici allegati.
Ritiene, dunque, che sussista la colpa grave del ricorrente, il quale, seppur inconsapevolmente, ha collaborato alla realizzazione della truffa, dapprima inserendo i dati nel link fraudolento e poi comunicando al truffatore i codici OTP necessari per autorizzare le operazioni.
In tal senso fa presente che i codici OTP sono stati generati da un Token Hardware, ossia un dispositivo fisico, che nel caso di specie è rimasto sempre in possesso del ricorrente.
Evidenza poi che gli sms ricevuti sembravano provenire dall'intermediario B e che il ricorrente non ha riflettuto su tale "macroscopica incongruenza". Inoltre, evidenzia come il cliente abbia ignorato l'alert relativo all'avvenuto cambio di indirizzo mail.
Sottolinea di aver posto in essere campagne informative nei confronti della propria clientela, al fine di evitare simili truffe, richiamando l'attenzione dei clienti soprattutto sull'obbligo di custodia dei codici di accesso che consentono l'utilizzo del servizio online.
Conclude evidenziando come il ricorrente sia stato vittima della ormai nota truffa dello smishing, che esula dalla responsabilità della banca nell'ipotesi in cui il ricorrente comunichi imprudentemente le credenziali di accesso all'home banking a terzi, versando così in colpa grave (richiama decisioni ABF).
Si costituisce l'intermediario B, il quale eccepisce il proprio difetto di legittimazione passiva, non essendo l'emittente della carta di debito, ma gestendone solo la funzionalità. Precisa che la carta in questione è stata emessa e collocata dall'intermediario A, titolare del rapporto contrattuale e di non aver alcun ruolo in relazione allo strumento di home banking.
Riguardo la tutela dei dati personali, eccepisce di adottare sistemi certificati da Enti Certificatori accreditati, di aver implementato le misure di sicurezza tecniche e organizzative ex art. 32 del Regolamento UE 679/2016 (GDPR) nonché di sottoporsi periodicamente ad un riesame delle misure di sicurezza adottate ai sensi dell'art. 3 del Regolamento Delegato 2018/389 da parte di un revisore esterno indipendente e qualificato. Infine, esclude di aver ceduto dati personali a terzi senza il consenso del ricorrente interessato.
Il ricorrente, in sede di repliche all'intermediario A, eccepisce anzitutto di non aver ricevuto la comunicazione relativa alla modifica dell'indirizzo email su cui ricevere gli avvisi delle operazioni, di cui non è fornita prova dalla resistente.
Lamenta la mancata adozione di misure volte ad impedire l'utilizzo dei propri numeri di telefono, la mancata attivazione di strumenti di alert o di blocco delle operazioni a fronte di anomalie e, soprattutto, la mancata attuazione della SCA.

Esclude la propria colpa grave, asserendo di essere stato tratto in inganno dalla circostanza che la telefonata pervenisse da un numero riconducibile all'intermediario e che l'operatore fosse a conoscenza di suoi dati sensibili.
Insiste, pertanto, per l'accoglimento del ricorso.
Il ricorrente, in sede di repliche all'intermediario B, contesta l'estraneità di quest'ultimo ai fatti in esame, in quanto l'SMS con il link fraudolento è pervenuto da un numero uguale a quello da quest'ultimo utilizzato per le comunicazioni con il cliente e che il sito civetta era riconducibile al predetto intermediario, di cui inseriva le credenziali di accesso.
Ribadisce come l'operatore telefonico fosse a conoscenza di dati che erano stati forniti solo all'intermediario B e che hanno reso possibile la realizzazione della truffa.
Ritiene, pertanto, infondata l'eccezione di difetto di legittimazione passiva sollevata dall'intermediario B, considerandolo solidalmente obbligato con l'intermediario A al risarcimento delle somme indebitamente sottratte.
L'intermediario A, in sede di controrepliche, conferma quanto affermato in sede di controdeduzioni e produce ulteriori log dai quali poter evincere l'utilizzo del sistema di doppia autenticazione; in particolare, la disposizione dei bonifici ha richiesto una doppia password OTP dinamica, una conoscibile solo dall'utente che effettua l'operazione (elemento di conoscenza) e l'altra generata dal Token Hardware in possesso dell'utente (elemento di possesso). Allega anche evidenze volte a provare l'avvenuto invio dell'email di modifica dell'indirizzo collegato al rapporto, diversamente da quanto affermato dal ricorrente.
Evidenzia inoltre che, da quanto affermato in sede di repliche, il sito civetta su cui il ricorrente si è autenticato era riconducibile all'intermediario B, mentre le credenziali inserite erano quelle relative all'Intenet banking dell'intermediario A.
Infine, chiede il rigetto del ricorso data la ormai notorietà diffusa di tale tipo di truffe.

DIRITTO

Il Collegio è chiamato a decidere su una controversia attinente all'accertamento di eventuali profili di responsabilità degli intermediari convenuti per l'esecuzione di operazioni non autorizzate e la conseguente richiesta di rimborso di somme relative ad operazioni disconosciute formulata dal ricorrente.
In via preliminare, va esaminata l'eccezione sollevata dal secondo intermediario resistente circa il proprio difetto di legittimazione passiva. L'eccezione è fondata. L'intermediario B eccepisce, infatti, la sua carenza di legittimazione passiva in quanto non sarebbe parte del rapporto contrattuale oggetto di contestazione, intrattenuto unicamente tra l'intermediario A e il ricorrente. Sostiene, inoltre, che, oltre a non essere emittente dello strumento di pagamento (carta di debito internazionale) tramite cui è stata perpetrata la frode, nemmeno ne è collocatore: lo strumento di pagamento sarebbe stato emesso e collocato dall'intermediario A, presso cui è acceso il conto corrente associato alla carta, mentre l'intermediario B è mero gestore della funzionalità della stessa. Specifica, inoltre, di non aver alcun ruolo in relazione allo strumento di home banking, messo a disposizione di parte ricorrente dal primo intermediario.
Il Collegio in proposito rammenta che secondo l'orientamento condiviso dai Collegi territoriali, in via generale – in ragione del rapporto contrattuale instaurato tra l'utente e il collocatore dello strumento di pagamento – sussiste la legittimazione passiva di quest'ultimo, con conseguente onere della prova sull'autenticazione delle operazioni contestate. Fa eccezione l'ipotesi in cui il PSP sia "mero" collocatore della carta: per accertare questo profilo si ha riguardo alla documentazione agli atti. A titolo esemplificativo, se la denominazione e il marchio dello strumento sono riconducibili esclusivamente all'emittente, si tratta di "mero" collocatore; se le previsioni contrattuali affidano al collocatore

il ruolo di riscontro all'utenza in caso di reclami, ovvero se il collocatore ha risposto al reclamo dell'utente senza segnalargli l'eventuale difetto di legittimazione passiva, non si tratta di "mero" collocatore.

Ciò premesso, il Collegio osserva che gli intermediari non hanno prodotto l'accordo di licenza stipulato, mentre depositano in atti copia del contratto relativo all'emissione della carta di debito oggetto di utilizzo fraudolento, in cui vengono descritti i rapporti tra i due intermediari. Dall'esame della documentazione prodotta, emerge che la carta di credito della ricorrente è stata emessa e collocata dal primo intermediario, mentre il secondo ha solo fornito dei servizi di gestione della carta al primo intermediario per incrementarne le funzionalità. Lo stesso contratto intercorso tra i due intermediari chiarisce espressamente la competenza del primo per ogni reclamo o ricorso dei clienti. Dall'analisi delle disposizioni contrattuali, si evidenzia inoltre che nella sezione dedicata ai reclami sono riportati esclusivamente i riferimenti dell'intermediario A. Il Collegio, inoltre, precisa che le operazioni di bonifico sembrano avvenute tramite disposizioni dal conto corrente acceso presso l'intermediario A, piuttosto che tramite carta.

Venendo al merito, le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018.

Si tratta, in particolare, di tre bonifici disposti da home banking, di cui il primo per € 59.000,00, il secondo per € 59.980,00 e il terzo per € 29.970,00 eseguiti in data 23/03/2023, per un totale complessivo di € 148.950,00. Le operazioni risultano dalla lista movimenti del conto corrente allegata dal ricorrente. Il ricorrente ha sporto denuncia all'A.G. il 23.03.2023, nella quale si ricostruiscono i fatti in modo analogo al ricorso.

Per quanto concerne l'autenticazione delle operazioni in questione, l'intermediario riferisce che gli ordini di bonifico per cui vi è contestazione, impartiti a mezzo di internet banking, sono stati validati attraverso un sistema di autenticazione forte a due fattori. Ricostruisce, in via generale, le modalità di:

- accesso all'Internet Banking per imprese: tramite browser/pc è necessario l'utilizzo congiunto della userid-password e del codice OTP a 6 cifre generato dal Token Hardware da inserire sul pc nel campo "login OTP";
- disposizione di un bonifico: è necessario l'utilizzo congiunto (dopo la preventiva autenticazione di accesso) del codice OTP, da digitare sul Token, generato a video dopo l'inserimento dell'operazione (elemento di conoscenza) e del codice OTP a 6 cifre generato dal Token Hardware, da digitare sul pc (elemento di possesso);
- modifica dei dati personali: è necessario l'utilizzo congiunto del codice OTP, da digitare sul Token, generato a video dopo l'inserimento dell'operazione di modifica (elemento di conoscenza) e del codice OTP a 6 cifre generato dal Token Hardware, da digitare sul pc (elemento di possesso).

A supporto di quanto affermato, in sede di controdeduzioni, produce la "guida utente" (cfr. all.1) che descrive la modalità operativa per l'utilizzo del token hardware sia per la fase di accesso all'Internet Banking, che per le disposizioni di bonifico.

Il Collegio osserva che, sia per le disposizioni di bonifico, sia per la modifica dei dati personali, l'intermediario qualifica come elemento di conoscenza, il primo dei codici OTP, quello che viene generato a video dopo l'inserimento dell'operazione di bonifico o della modifica dei dati personali.

Ciò trova conferma nella allegata guida in cui si precisa che, per le disposizioni dei bonifici, tale OTP viene generato da un codice composto dalle ultime sei cifre dell'IBAN destinatario del bonifico e dall'importo senza decimali del bonifico stesso. In merito all'utilizzo dell'OTP quale elemento di conoscenza, il Collegio rappresenta che, alla stregua di quanto indicato

nell'Opinion EBA 2019, l'OTP così generato non integra un valido elemento di conoscenza, poiché non si tratta di un codice che soltanto il cliente conosce.
Orbene, anche sulla base della già richiamata Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, deve ritenersi che l'utilizzo di una password OTP, generata a video dopo l'inserimento dell'operazione, non possa essere ritenuta un valido fattore di conoscenza; il che non consente di affermare che le operazioni di pagamento siano state compiute all'interno di un sistema adeguatamente presidiato da un sistema di autenticazione forte.
Per completezza, il Collegio aggiunge che l'intermediario, in sede di controdeduzioni, ha precisato che le disposizioni di bonifico sono state eseguite a seguito di un secondo accesso alla piattaforma di Internet Banking avvenuto alle ore 13.23, tramite dispositivo mobile.
In particolare, dai logs estratti dal sistema informatico dell'intermediario relativi al periodo 23/03/2023– 24/03/2023 e prodotti in sede di controdeduzioni si evince che:

- alle 13:16 un'attività di login da un indirizzo IP diverso da quello precedentemente utilizzato presumibilmente dal ricorrente;
- alle 13:18 un'autorizzazione concernente i dati personali;
- alle 13:23 una nuova attività di login da un canale mobile;
- alle 13:33 un'autorizzazione di un bonifico di € 59.000
- alle 13:40 una seconda autorizzazione di un bonifico di € 59.980
- alle 13:44 una terza autorizzazione di un bonifico di € 29.970

In sede di controrepliche, l'intermediario allega ulteriori log volti a provare l'utilizzo del sistema di doppia autenticazione nelle varie fasi.
Il Collegio rileva, tuttavia, che dall'esame dei predetti log l'intermediario descrive e dà evidenza solamente delle modalità del primo accesso, avvenuto alle ore 13:16 tramite pc; mentre non chiarisce le modalità del citato secondo accesso che, tra l'altro, da quanto asserito, sarebbe avvenuto dal dispositivo mobile dei truffatori, quindi previo enrollment dello stesso. Manca, in altri termini, qualsiasi riferimento all'operazione di enrollment del Token Software sul device dei truffatori (cfr. Collegio di Roma, dec. n. 688/22), e, dunque, la prova dell'impiego della SCA nella fase di onboarding.
Difettando, dunque, la dimostrazione oggettiva della procedura di autenticazione e autorizzazione che la banca sostiene avere adottata nella fattispecie in esame, non è possibile ritenere che le operazioni di pagamento in questione siano state compiute all'interno di un sistema adeguatamente presidiato, secondo gli standard di sicurezza definiti dalla regolamentazione pro tempore vigente in materia, come declinati dall'EBA negli orientamenti del 21 giugno 2019 sull'autenticazione forte.
Alla luce di queste evidenze, deve, pertanto, essere riconosciuto il diritto del ricorrente ad ottenere la ripetizione del controvalore delle operazioni disconosciute.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario A corrisponda al ricorrente la somma di € 148.950,00.
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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI