COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) GENOVESE	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO ACCETTELLA

Seduta del 11/11/2022

FATTO

1. L'odierno ricorrente riferisce di aver subito una frode informatica in data 05/10/2020. Anche a mezzo della denuncia acclusa, espone quanto segue. Nel pomeriggio del 5/10/2020 è stato contattato sul suo numero di cellulare da un sedicente operatore dell'intermediario convenuto A in merito alla necessità di eseguire un aggiornamento della *privacy*. A tal fine, l'operatore gli ha chiesto conferma dei suoi dati anagrafici e del suo numero di cellulare. Dopo averne acquisito i dati, il truffatore lo invitava a disinstallare dal telefono cellulare l'applicazione mobile dell'intermediario A e a reinstallarla dopo le ore 19:00, orario in cui avrebbe ricevuto un'altra chiamata dalla banca. Il cliente ha seguito le indicazioni e ha eliminato l'*app*. Intorno alle ore 19:30, non avendo ricevuto alcuna chiamata, ha visto sul cellulare un messaggio in entrata da parte del gestore telefonico dal seguente tenore: "Come da tua richiesta stiamo procedendo al blocco della linea per furto". Ha subito contattato il servizio clienti del gestore di telefonia mobile, apprendendo che era stata effettuata una richiesta di blocco della sua linea per furto. Disconosceva la richiesta e l'operatore procedeva a ristabilire la linea. La mattina seguente l'odierno ricorrente ha reinstallato l'applicazione dell'intermediario A, ma, poiché non riusciva ad accedervi, ha chiamato il Servizio Clienti, venendo a conoscenza dell'esecuzione, nella giornata del 5/10/2020, di un bonifico di euro 14.900,00 in favore di un soggetto sconosciuto, del quale gli veniva fornito il numero di telefono.

Parte ricorrente rileva che l'intermediario A ha dato esecuzione al bonifico senza porre in essere tutte le misure idonee a garantire l'effettiva riconducibilità dell'operazione alla volontà del cliente. Aggiunge che, nell'erogare il servizio di *home banking*, la banca deve garantire uno standard di sicurezza dei pagamenti adeguato a precludere l'accesso a soggetti non abilitati, con la diligenza dell'accorto banchiere. Osserva ancora che la normativa di riferimento pone a carico della banca l'obbligo di risarcire il correntista truffato, a meno che questa non dimostri la piena legittimità della operazione contestata, e rileva, nel caso di specie, la mancanza di autorizzazione dell'operazione di pagamento, non essendo l'ordine di bonifico in alcun modo riconducibile al ricorrente, che l'ha subito contestato e ha sporto regolare denuncia. Sostiene altresì che l'intermediario A, seppure tempestivamente informato della truffa, non si è adoperato per la revoca del bonifico non autorizzato, riuscendo a recuperare solo l'importo euro 3.000,50. Afferma che l'importo risulta ancora trattenuto dall'intermediario convenuto B, presso cui è incardinato il conto del beneficiario, che ha opposto un ingiustificato rifiuto nonostante la sottoscrizione, da parte del ricorrente, della lettera di manleva come richiesta.
Parte ricorrente, nei confronti dell'intermediario A, chiede il risarcimento del danno pari all'importo del bonifico di euro 14.990.00, oltre interessi a far data dal 16/12/2020, data della prima richiesta di rimborso, nonché il risarcimento del danno patrimoniale e non patrimoniale da quantificarsi almeno in euro 5.000,00. Nei confronti dell'intermediario B chiede l'immediata restituzione della somma di euro 3.000,50 ancora presente sul conto corrente del beneficiario, oltre agli interessi a far data dalla prima richiesta di restituzione e comunque dall'ultimo ingiustificato rifiuto dell'11/06/2021, nonché il risarcimento del danno patrimoniale e non patrimoniale che si quantifica in almeno 1.000,00 euro.
2. L'intermediario A si costituisce e deduce che il ricorrente è titolare del conto corrente n. *584 al quale è collegato il servizio di *home banking*, che consente al cliente di effettuare le operazioni di *inquiry* e dispositive sui conti correnti a lui riferibili utilizzando il telefono via *app* o via Internet sul sito dell'intermediario. Osserva che l'*home banking* prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte" basato sui seguenti fattori: i) inserimento delle credenziali di accesso (numero cliente + PIN), per effettuare il *login*; ii) PIN + *One Time Password* /OTP per disporre le operazioni. L'OTP è generata dalla specifica funzionalità dell'*app* (*Mobile Token*). Parte resistente sostiene che l'operazione risulta correttamente autenticata, registrata e contabilizzata attraverso un sistema di autenticazione "forte", senza che sia emerso alcun malfunzionamento o compromissione dei sistemi di sicurezza predisposti dall'intermediario. Afferma che la truffa è stata verosimilmente perpetrata con "SIM swapping", che prevede il trasferimento da una *SIM card* a un'altra del numero di telefono della vittima. Sostiene che il frodatore che si appropria del numero di cellulare di un cliente deve conoscere: il numero di cellulare associato con il nominativo del cliente, carpito precedentemente mediante *phishing*; i dati anagrafici del titolare dell'utenza telefonica per chiedere la sostituzione della SIM; il numero cliente (ID) e il PIN per accedere all'*home banking* una volta ottenuta la SIM. Il telefono del cliente cessa di avere linea, una volta attivata la nuova SIM sul *device* del frodatore, sul quale questi scarica la *app* dell'intermediario e, dall'*app*, il *Mobile Token*. Il malvivente è così in grado di effettuare tutte le operazioni, ricevendo gli *SMS alert* ed ogni altra comunicazione della banca direttamente sul proprio telefono. Parte resistente precisa che non è possibile con la conoscenza delle sole credenziali statiche (numero cliente e PIN) accedere al *Mobile Token*, per la cui attivazione è richiesto il codice (OTP) inviato dalla banca sul telefono del cliente (presente in anagrafica), e che la variazione del numero di telefono in anagrafe viene sempre notificata al vecchio numero del cliente con SMS, email, messaggio nella *message box* e notifica *push*. Rileva che il servizio di *SMS alert* era ed è tuttora attivo sul

profilo del ricorrente e che, nel caso in esame, i messaggi del 5/10/2020, relativi al bonifico oggetto del ricorso, non sono pervenuti al ricorrente a causa del blocco della SIM. L'intermediario sostiene di informare periodicamente la clientela sulle varie tipologie di frode diffuse *online*, tra le quali vi è la "sim swap fraud" in oggetto, per la cui riuscita è necessaria la collaborazione del cliente nel fornire ai frodatori le credenziali di accesso all'*home banking*. Aggiunge che, se il cliente avesse immediatamente contattato l'intermediario A, a fronte del blocco telefonico, forse il bonifico in questione sarebbe stato bloccato. Dalle verifiche sulle chiamate giunte al Centro Clienti risulta "una chiamata del 05/10/2020 alle ore 19:31 proveniente dal 328***3429 e diretta verso lo 06**60. Il tempo di permanenza su IVR è stato di 1 minuto e 43 secondi, il cliente ha agganciato la chiamata dopo aver effettuato la scelta 6". Parte resistente evidenzia infine la lacunosità della narrazione dei fatti contenuta sia nella denuncia che nel ricorso.
L'intermediario A chiede pertanto il rigetto del ricorso.
3. L'intermediario B ha prodotto, in luogo delle controdeduzioni, un accordo transattivo sottoscritto dai ricorrenti, a fronte della rinuncia alle domande proposte nei suoi confronti. Chiede pertanto che sia dichiarata cessata la materia del contendere.
4. In sede di repliche, parte ricorrente insiste nell'accoglimento della domanda nei confronti dell'intermediario A e, alla luce delle difese avversarie, invoca la responsabilità dell'intermediario resistente quale titolare del trattamento dei dati personali dei clienti. Richiama l'art. 15 del Codice della *Privacy*, a norma del quale chiunque cagioni un danno ad altri per effetto di un illecito trattamento dei dati personali è tenuto al risarcimento, ai sensi dell'articolo 2050 c.c.

DIRITTO

1. La presente controversia ha ad oggetto il disconoscimento di un bonifico *online* di euro 14.990,00, effettuato a valere sul conto corrente del ricorrente.
Preliminarmente, il Collegio dichiara cessata la materia del contendere con riferimento all'intermediario B.
Al riguardo, si rileva che l'intermediario B ha fatto pervenire, in luogo delle proprie controdeduzioni, copia di un accordo transattivo sottoscritto dalla parte ricorrente e quest'ultima, tramite il proprio procuratore, ha confermato l'avvenuto pagamento delle somme oggetto di transazione e la cessazione della materia del contendere in relazione alla domanda proposta nei confronti del medesimo intermediario.
2. Venendo alla posizione dell'intermediario A, si osserva che l'operazione fraudolenta è avvenuta in data 05/10/2020 e, dunque, risulta essere stata effettuata nel vigore della Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta *PSD* 2 - *Payment Services Directive* 2), recepita con il d.lgs. n. 218 del 2017 del 15/12/2017, entrato in vigore in data 13/01/2018, che modifica in più punti il d.lgs. n. 11 del 2010.
Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-*bis*, commi1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 *che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri*. Il regolamento, ai

sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13/03/2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14/09/2019.

3. La normativa vigente fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un cd. "sistema di autenticazione forte". Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis* del predetto d. lgs. n. 11/2010, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

Il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

4. Qualora il prestatore di servizi di pagamento abbia adottato un sistema di autenticazione forte del cliente, si ricade nelle fattispecie regolate dai commi terzo e quarto dell'art. 12 d.lgs. n. 11/2010. In base al primo, "salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita". Mentre, ai sensi del secondo, "qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3". A sua volta, l'art. 7 del decreto prevede gli obblighi che l'utente dei servizi di pagamento deve osservare in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate. In particolare, il comma primo, lett. a) impone a costui di "utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso", mentre il comma secondo dispone che, ai fini del corretto utilizzo dello strumento di pagamento, "l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate". Il Provvedimento della Banca d'Italia del 5/07/2011 di *Attuazione del Titolo II del decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti)* ribadisce e precisa le suddette previsioni normative.

Va altresì richiamatala previsione dell'art. 10, comma 1, d.lgs. n. 11/2010 [così come introdotto dall'art. 2, comma 10, lettera c) d.lgs. n. 218/2017], in relazione alla *prova di autenticazione ed esecuzione delle operazioni di pagamento*: "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita (…), è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". Il comma secondo della medesima norma precisa che: "Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

5. Nel caso di specie, sulla base di quanto dichiarato da entrambe le parti, può considerarsi pacifico che la frode subita dal ricorrente sia stata perpetrata con la tecnica combinata del *vishing* e del c.d. *sim swapping*. In dettaglio, il ricorrente è stato contattato da un sedicente operatore del servizio clienti dell'intermediario, il quale, per procedere a un presunto aggiornamento della *privacy*, ha carpito le credenziali di accesso all'applicazione di *home banking* dell'intermediario e ha indotto il cliente a disinstallarla dal proprio *device*. Il frodatore ha ottenuto, sempre tramite *vishing*, anche il numero di cellulare associato con il nominativo del cliente e i suoi dati anagrafici, per chiedere la sostituzione della SIM. A quel punto, l'utenza telefonica del ricorrente è stata bloccata "per furto" ad opera del frodatore e quest'ultimo ha installato l'applicazione dell'intermediario sul proprio *device*, attivando il *Mobile Token*. Il frodatore ha quindi effettuato l'accesso all'*home banking* e ha disposto il bonifico disconosciuto, ricevendo sulla SIM duplicata i codici OTP e gli *SMS alert*.

6. Al riguardo, è orientamento condiviso dai Collegi territoriali dell'ABF quello secondo cui "*la sostituzione della sim card va (…) equiparata alla mancanza di autenticazione dell'operazione di pagamento*", ai sensi dell'art. 10 del d.lgs. n. 11/2010. In particolare, diversamente da altre fattispecie – come quella nota con l'espressione *man in the browser* – in cui la valutazione della vicenda rientra nell'ambito dell'art. 12 d.lgs. n. 11/2010 e riguarda i profili di colpa dell'utente, nei casi di *sim swap fraud* l'operazione di pagamento non può ritenersi "regolarmente autenticata" e la fattispecie va dunque affrontata alla luce della previsione di cui all'art. 10 del menzionato decreto.

La *sim swap fraud* si caratterizza per essere una fattispecie nella quale, dopo il furto di identità e la captazione dei dati di accesso relativi al servizio di *home banking*, la sim del cliente viene duplicata o sostituita dai malfattori, in maniera tale da deviare su una diversa utenza telefonica i messaggi provenienti dalla banca contenenti i codici autorizzativi delle operazioni *online*. Tale particolare modalità di sottrazione dell'identità (telefonica) del cliente è destinata ad esautorare la funzionalità protettiva del sistema di autenticazione multifattoriale, pur in astratto predisposto dall'intermediario, essendo l'utenza telefonica – modificata dai malfattori – il naturale canale di ricezione dei codici OTP. In particolare, viene meno il requisito dell'indipendenza dei fattori di autenticazione, in quanto "*la violazione di una singola misura di sicurezza ha compromesso anche l'affidabilità dell'altra, quando, al contrario, la piena operatività del sistema di autenticazione multifattore si fonda sull'indipendenza tra le singole misure di sicurezza*" (cfr., tra gli altri,

Collegio di Roma, decisione n. 19544/2020 e decisione n. 11777/2019; Collegio di Milano, decisione n. 1066/2019).
In conseguenza della sostituzione della SIM dell'utenza telefonica associata al servizio di *home banking*, si deve ritenere che manchi l'autenticazione dell'operazione di pagamento, ai sensi e per gli effetti dell'art. 10 d.lgs. n. 11/2010, e che parte ricorrente abbia diritto al rimborso integrale, da parte dell'intermediario A, della somma sottratta all'esito dell'operazione fraudolenta, al netto dell'importo recuperato e già corrisposto dall'intermediario B.
7. Parte ricorrente chiede, altresì un risarcimento di euro 5.000,00 a titolo di danni patrimoniali e non patrimoniali subiti. Tuttavia, non fornisce prova dell'ulteriore danno che afferma di aver subito, oltre a quello consistente nella sottrazione della somma oggetto del bonifico fraudolento.
In linea con l'orientamento giurisprudenziale consolidato, l'ABF esclude la risarcibilità di lesioni integranti meri disagi o fastidi e ritiene non sussistente un danno *in re ipsa*, dovendo essere, comunque, dimostrata dalla parte ricorrente la sua concreta esistenza (cfr., *ex multis*, Collegio di Roma, decisione n. 21194/2018).
Una simile pretesa non può pertanto essere accolta.

PER QUESTI MOTIVI

Il Collegio dichiara cessata la materia del contendere nei confronti dell'intermediario B.
Dispone che l'intermediario A corrisponda alla parte ricorrente la somma di euro 12.022,95 oltre interessi legali dalla richiesta al saldo. Respinge nel resto.
Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario A corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura.
Prende atto che alla parte ricorrente è stata rimborsata la somma di Euro 20,00 (venti/00) versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA