COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore (MI) FRANCESCO DENOZZA

Seduta del 18/04/2024

FATTO

Per la descrizione analitica dell'oggetto, il ricorrente rinvia ai documenti in atti, documenti in cui si afferma che:

- il cliente è un operario che guadagna meno di euro 2.000,00 al mese, con un minore a carico e versa i propri risparmi sul c/c n. 43***00 della banca convenuta (intermediario A);
- il contratto è stato associato a un numero telefonico (334*****17) comunicato dal cliente;
- c'è una partnership tra gli intermediari coinvolti nell'odierno procedimento, come da comunicato congiunto del 27/03/2023, per cui è possibile gestire il c/c accedendo al sito dell'APP della banca (intermediario A) e autenticare le operazioni inserendo le credenziali ricevute per il tramite dell'intermediario B;
- in data 26/07/2023 il cliente riceveva alcuni SMS nella chat ufficiale dell'intermediario B, riportante come mittente il nome di quest'ultimo;
- i messaggi apparivano autentici in quanto formulati in modo pressoché identico a quelli genuini;
- l'SMS conteneva un avviso con riferimento alla richiesta di una spesa di Euro 999,00: qualora il ricorrente avesse voluto disconoscere tale operazione avrebbe dovuto cliccare sul link riportato nel corpo del messaggio;

- il cliente procedeva a cliccare sul link, venendo reindirizzato a un sito in cui poteva selezionare la possibilità di essere ricontattato da un operatore dell'intermediario B;
- il ricorrente, poco dopo, riceveva una chiamata dal numero 023*****180 da un soggetto qualificatosi come operatore antifrode che gli confermava la disposizione di un'operazione di acquisto, a Madrid, dal valore di Euro 4.990,00;
- il cliente disconosceva l'esecuzione del bonifico e chiedeva delucidazioni così da poter bloccare sia il bonifico che il c/c;
- non essendo possibile procedere al blocco richiesto dal cliente, l'operatore gli comunicava che avrebbe ricevuto dei codici;
- in data 27/07/2023, alle ore 15:36, giungeva sull'utenza del cliente un ulteriore messaggio all'interno della chat ufficiale dell'intermediario B, che lo invitava a cliccare su un link e a inserire i codici di accesso. Il ricorrente procedeva seguendo tali istruzioni;
- poco dopo il ricorrente riceveva una mail (genuina) da parte dell'intermediario A in cui veniva informato della richiesta di attivazione di un dispositivo, associato al suo numero di cellulare, da finalizzare con un codice contenuto nel corpo della mail;
- il cliente inseriva il codice ricevuto via email sull'APP e successivamente, tramite una mail ulteriore, veniva a conoscenza che era stato disposto un bonifico a suo nome di Euro 4.990,00;
- contattato nuovamente dall'operatore, gli veniva comunicato di inserire nuovamente i codici di accesso in APP;
- in data 28/07/2023 riceveva due mail dall'intermediario A in cui veniva a conoscenza che erano stati attivati altri due dispositivi al suo account, collegati al suo numero di cellulare (anche tali mail avevano dei codici da inserire in APP per finalizzare l'attivazione dei device, che il cliente procedeva a inserire);
- in data 01/08/2023 il cliente riceveva un'ulteriore chiamata dal sedicente operatore (che comunicava altri codici) e altre due mail che lo informavano della disposizione di due bonifici verso due soggetti diversi pari a un importo di Euro 4.990,00 ciascuno;
- in data 03/08/2023 si recava in filiale per chiedere spiegazioni e gli veniva confermata la sottrazione di un importo di Euro 14.970,00;
- il cliente procedeva a disconoscere le operazioni e a presentare denuncia;
- inoltrava reclamo in dara 26/09/2023 seguito da riscontro negativo;
- la frode è riconducibile allo *spoofing*;
- la banca non ha rispettato le condizioni di autenticazione forte sancite dalla normativa di riferimento;
- non è ravvisabile colpa grave del cliente in quanto i messaggi civetta sono giunti nella chat ufficiale e sono stati susseguiti da mail genuine;
- la banca ha preso in carico le richieste di attivazione di molteplici dispositivi senza adottare alcuna misura volta a mitigare il rischio di frode;
- le domande di attivazione del secondo e del terzo dispositivo, associati all'account e al numero del cliente, sono state prese in carico dalla banca dopo un solo giorno dalla richiesta di attivazione del primo dispositivo a distanza di pochi minuti l'una dall'altra;
- gli importi dei bonifici sono appena sotto la soglia di controllo e presentano delle causali simili e "*improbabili*" e "*comportavano un esborso del tutto fuori linea dalle possibilità economiche e dalla pregressa operatività del ricorrente*";
- anche l'intermediario B non ha utilizzato un sistema adeguato alla prevenzione della frode informatica, infatti i codici OTP non sono sicuri se inviati via SMS (essendo intercettabili).

Chiede la condanna degli intermediari alla restituzione della somma di E, 14.970,00 oltre interessi dal dovuto al saldo.

L'intermediario A espone:

- il cliente è titolare del c/c n.***800, dove sono attivi i servizi di banca;
- al momento dell'attivazione del servizio home banking, il ricorrente ha fornito i contatti associati alla sua utenza, mai modificati;
- tuttavia, è stata registrata una modifica dell'anagrafica cliente;
- il cliente ha prodotto copia del messaggio (apparentemente proveniente dall'intermediario B), delle e-mail genuine relative all'OTP e dell'informativa relativa all'attivazione della nuova APP;
- non è stata allegata copia della schermata relativa alle telefonate (ricevute da un presunto operatore dell'intermediario B) provenienti dal numero 023****180, peraltro non riconducibile all'intermediario A;
- dalla lettura della denuncia e del reclamo si evince che il cliente ha tenuto una condotta negligente reiterata tra il 26/07/2023 e il 03/08/2023 (giorni in cui sarebbe stata perpetrata la truffa);
- solamente in data 03/08/2023 sarebbe stato informato dalla banca che erano stati eseguiti e autorizzati n. 3 bonifici di Euro 4.999,00;
- il cliente aveva seguito la procedura proposta dal sedicente operatore dell'intermediario, credendo di bloccare il proprio conto ovvero annullare/stornare presunte operazioni di bonifico nell'arco di 2 giornate consecutive;
- il cliente disconosceva verbalmente le operazioni richiedendo la restituzione dell'importo;
- la banca inviava le richieste di recall con esito negativo e provvedeva a bloccare l'utenza home banking;
- in data 28/08/2023 la banca forniva riscontro negativo alla richiesta di rimborso relativa alle transazioni disconosciute, di importo pari a Euro 14.970,00, poiché avvenute regolarmente tramite internet banking;
- in data 26/09/2023 il cliente ha inoltrato reclamo, riscontrato negativamente in data 17/10/2023;
- il sistema adottato dall'intermediario A non si relaziona in alcun modo con l'intermediario B, che gestisce autonomamente le proprie carte di pagamento;
- c'è stata un'attiva collaborazione tra il cliente e il terzo frodatore tenuto conto che la truffa si è compiuta nell'arco di 7 giorni (dal 26/07 al 03/08) e che il cliente ha riconosciuto di aver ricevuto comunicazioni genuine tanto in relazione alla richiesta di attivazione di una nuova licenza OTP, quanto in relazione all'informativa relativa alla disposizione delle operazioni di pagamento;
- il cliente ha comunicato i propri codici;
- il cliente avrebbe dovuto sospettare la non genuinità del messaggio infatti, il testo si presentava in forma sgrammaticata e il link non era riconducibile all'intermediario B. Ad ogni modo, in base a sue dichiarazioni, avrebbe cliccato sul link e inserito/comunicato i codici più volte in giorni differenti (nonostante fosse stato avvertito di non comunicare a terzi);
- nonostante gli accordi commerciali tra gli intermediari convenuti si precisa che l'intermediario B non può richiedere l'accesso all'Internet banking del cliente;
- il cliente avrebbe ricevuto una sola comunicazione in cui, apparentemente, l'intermediario B gli avrebbe riferito la proceduta da seguire per disconoscere un pagamento; tuttavia non era specificato alcun dettaglio (diversamente dal regime di trasparenza prediletto dalla banca), il che avrebbe dovuto insospettire;

- è possibile presumere che il cliente, seguendo le istruzioni del frodatore, abbia disinstallato la APP DMobile dal proprio dispositivo consentendo, contestualmente, al frodatore di effettuare simultanea attivazione della medesima APP su un nuovo dispositivo, non in possesso del cliente già dalla data del 27/07;
- non era possibile che un operatore dell'intermediario B chiedesse, legittimamente, la disinstallazione di un'applicazione indispensabile per i clienti fruitori dell'Internet Banking dell'intermediario A;
- il cliente non ha prestato attenzione ai messaggi di notifica esecuzione dei bonifici che, contestualmente, riceveva all'autorizzazione di ciascuna operazione;
- il cliente non si è insospettito neppure ricevendo 3 comunicazioni mezzo mail dalla banca con le quali veniva avvertito che si stava attivando una nuova licenza smartOTP;
- è stata provata la corretta registrazione ed esecuzione dei bonifici informatici assolvendo all'onere probatorio ex art. 10 comma 1 D.lgs. 11/2010;
- è stato il cliente ad autorizzare le operazioni.

Chiede la reiezione del ricorso o in subordine l'accertamento di un concorso di colpa.

L'intermediario B espone:

- la truffa si è svolta secondo uno schema tipico a seguito della ricezione di un SMS e di una successiva chiamata del sedicente operatore, in cui pare chiaro l'atteggiamento collaborativo (anche se inconsapevole) del ricorrente, autenticatosi su un sito fake con le proprie credenziali;
- nessuna operazione contestata è stata conclusa con carte di pagamento N*** né è stata aperta alcuna disputa tramite il servizio clienti;
- eccepisce la carenza di legittimazione passiva specificando di non aver alcuna relazione con lo strumento di home banking messo a disposizione dall'intermediario A;
- l'intermediario scrivente non avrebbe svolto alcuna funzione rispetto a un rapporto contrattuale in cui le parti coinvolte sarebbero il cliente e l'intermediario A;

Chiede il non accoglimento del ricorso e l'accertamento dell'assenza della sua legittimazione passiva.

Il cliente osserva che la prolissità e la quantità di documentazione prodotta dall'intermediario A sarebbe tesa a distogliere l'attenzione dagli elementi decisivi.
Ad ogni modo, precisa che la ricostruzione dei fatti e la perizia allegata confermerebbero la ricostruzione proposta dal ricorrente:

- la banca ha acconsentito all'attivazione e disattivazione dell'l'APP per almeno 3 volte, su due dispositivi diversi, in un arco temporale ristretto, senza sospendere il servizio di home banking, neppure a fronte di bonifici aventi un importo leggermente inferiore (Euro 4.999,00) alla soglia di controllo (di Euro 5.000,00);
- l'operatività descritta dalla banca avrebbe dovuto destare sospetti anche perché è lo stesso intermediario a riferire di "*elementi di evidente anomalia*"; pertanto, non si comprende il motivo per cui la banca non abbia adottato alcun presidio di sicurezza;
- non viene fornita alcuna prova della condotta colposa del cliente e l'onere probatorio non può essere assolto mediante la mera produzione di log informatici;
- il cliente era impreparato a una frode così sofisticata e ha agito in buona fede.

Con riferimento all'intermediario B, la circostanza che questo non abbia alcun collegamento con i servizi dell'Internet Banking dell'intermediario A è contraddetta dal sito della banca; inoltre, è stata allegata schermata della telefonata ricevuta dal presunto

operatore. In particolare, la chiamata sarebbe pervenuta da un numero di telefono (023****80) riconducibile all'intermediario B (sebbene come numero fax). Inoltre:

- l'eccezione di carenza di legittimazione passiva è inconferente e infondata perché il sito della Banca indica, chiaramente, che tra gli intermediari vi sia una collaborazione;
- nel corso dell'anno in cui ha subito la truffa, l'intermediario B avrebbe inviato al cliente SMS autentici e genuini contenenti codici da utilizzare nell'ambito delle operazioni da lui richieste per cui, la ricezione dei messaggi (poi rivelatasi truffaldini) da parte dello stesso, non avrebbe potuto destare alcun sospetto;
- le misure messe in atto non si sono dimostrate efficienti a prevenire le frodi, come quella oggetto dell'odierno procedimento;
- è onere dell'intermediario fornire prova della frode, del dolo o della colpa grave dell'utente;
- l'intermediario B non dispone di alcun meccanismo idoneo a identificare e prevenire comportamenti anomali.

L'intermediario A contesta integralmente il contenuto delle difese formulate dal ricorrente, precisando che:

- non sussiste alcuna responsabilità in capo alla banca, che ha adottato un sistema di autenticazione forte per effettuare le operazioni dispositive tramite Internet banking;
- nel caso di specie, il presidio di sicurezza è stato violato a seguito della cooperazione attiva del cliente;
- il cliente dovrebbe produrre copia dell'SMS civetta, della schermata relativa alle telefonate e delle mail genuine ricevute dall'intermediario A;
- è stata ricevuta chiamata solo dal numero 023*** riconducibile esclusivamente all'intermediario B (coerentemente con quanto dichiarato dal cliente);
- qualora la banca avesse ritenuto di dover contattare il cliente per vie brevi, la chiamata sarebbe stata effettuata con il numero della filiale di riferimento del cliente (che ha un numero diverso);
- non si sarebbe verificato alcuno *spoofing* in quanto il numero riportava come mittente apparente l'intermediario B;
- l'intermediario B essendo il gestore delle carte di pagamento, non aveva alcun titolo per richiedere al cliente di inserire credenziali personali, a lui solo note, per accedere al c/c intrattenuto con l'intermediario A, che cura l'accesso al proprio sistema di home banking;
- per una fattispecie analoga il Collegio di Roma (decisione n.0012883/23 del 19/12/2023) ha integralmente rigettato il ricorso del cliente;
- il cliente non avrebbe dato rilevanza alle comunicazioni inviate dalla banca, con cui sarebbe stato avvertito del fatto che era in atto una richiesta di attivazione per una nuova licenza smart OTP (per un caso analogo è stata richiamata la decisione del Collegio di Bologna, n. 2593/24, con cui il ricorso è stato rigettato);
- in precedenti pronunce l'ABF ha dichiarato la conformità del sistema di autenticazione dell'intermediario A alla normativa di riferimento.

DIRITTO

L'intermediario B eccepisce, preliminarmente, la propria carenza di legittimazione passiva facendo presente che le parti del contratto sono il cliente e l'intermediario presso cui è

acceso il conto corrente sul quale sono regolate le operazioni di bonifico effettuate tramite l'home banking.
L'eccezione appare fondata. In effetti le operazioni contestate consistono in tre bonifici che non sembrano avere coinvolto l'operatività della carta e rispetto ai quali l'intermediario B sembra non rivestire alcuna posizione giuridica attiva rilevante, essendo stato un puro riferimento utilizzato dai truffatori per rendere maggiormente credibili gli artifici da essi posti in essere.
Venendo alle operazioni contestate si tratta come già detto di quattro bonifici effettuati in giorni diversi tra il 27/07/ 2023 e il 02/ 08/ 2023 per un importo complessivo di E 14.970,00
È in atti la denuncia presentata in data 03/08/2023, in cui il cliente precisa che:

- in data 26/07/2023 alle ore 19:35 riceveva una notifica alert in cui veniva informato di una spesa di Euro 999,00 che poteva essere disconosciuta cliccando sul link riportato nel corpo del messaggio;
- cliccato il link, veniva poco dopo contattato da un soggetto qualificatosi come operatore dell'intermediario B al numero 023****80;
- il soggetto riferiva, in realtà, che era stata addebitata una spesa di Euro 4.990,00 per l'acquisto di un orologio a Madrid;
- non avendo posto in essere quella transazione, il cliente chiedeva delucidazioni sulle modalità adeguate per procedere al blocco del conto;
- secondo le istruzioni del sedicente operatore, il ricorrente avrebbe dovuto ricevere dei codici tramite email (da inserire solamente dopo la ricezione di una telefonata che sarebbe pervenute nell'arco delle 24h successive);
- tuttavia, tra i codici ricevuti vi erano anche i dettagli di un bonifico eseguito;
- in data 27/07/2023 non essendo stato ricontattato avrebbe tentato l'accesso al conto con i vecchi codici e, nell'istante in cui stava per cliccare, riceveva la telefonata dell'operatore che comunicava che la procedura di storno dell'operazione di pagamento non era andata a buon fine poiché il cliente aveva tentato di accedere al conto inserendo i vecchi codici e pertanto avrebbe dovuto ripetere la procedura da capo e attendere 24 ore;
- procedeva a ripetere l'operazione e restava in attesa fino al 1/08/2023 quando veniva contattato nuovamente telefonicamente e gli venivano comunicati dei nuovi codici da inserire al fine di riattivare il conto soltanto dopo aver atteso ulteriori 24 ore;
- nel mentre riceveva una mail connotata dai dettagli di pagamento di un bonifico di Euro 4.999,00;
- il giorno seguente, in data 02/08/2023, senza essere ricontattato riceveva una mail relativa a un altro bonifico dal medesimo importo dei precedenti, avente, però, beneficiario diverso;
- recatosi presso l'istituto bancario, apprendeva di aver subito una truffa di Euro 14.970,00 e procedeva a disconoscere i 3 bonifici conclusi in suo nome.

L'intermediario afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate, e produce documentazione informatica a supporto.
In via preliminare si osserva che il servizio "smartotp" è stato attivato 3 volte, prima su un *device*, poi su un altro e poi di nuovo sul primo. Ogni attivazione è stata preceduta da relativa disattivazione.
L'intermediario rileva che alle ore 15:40:48 del 27/07/2023 è stata attivata una nuova licenza "*smartotp*", presumibilmente dal terzo truffatore (sul proprio dispositivo Android), Precisa che l'app può essere installata su un unico dispositivo mobile per volta, sicché l'attivazione dell'app/licenza smart OTP sul nuovo dispositivo è stata preceduta dalla disinstallazione della app sul device del cliente. La licenza "smartotp" è stata poi

disattivata per essere attivata su un dispositivo diverso. Tuttavia, alle ore 20:07:54, del 28/07/2023, la licenza "smartotp" è stata riattivata sul primo dispositivo.
Quanto all'attivazione dello smartphone, l'intermediario, nella legenda, spiega che il processo di *enrollment* prevede sempre inserimento di UTENZA + PASSWORD + OTP ricevuto via e-mail + OTP ricevuto via SMS. In data 27/07/2023 e in data 28/07/2023, è stata eseguita l'attivazione di un nuovo device da IP che è lo stesso utilizzato per effettuare l'accesso e disporre la transazione.
Si rileva però al riguardo che non vi è evidenza dell'inserimento di Utenza + Password
Quanto alle operazioni contestate si rileva che le operazioni sono avvenute con modalità analoghe e che ciascuna operazione è stata preceduta da un accesso all'Internet Banking del cliente tramite APP dal dispositivo su cui, previamente, è stata attivata la licenza "smartotp".
Dall'esame del complesso delle produzioni dell'intermediario sembra emergere che, con riferimento all'*enrollment* del nuovo dispositivo, è presente evidenza della validazione tramite OTP (elemento di possesso), ma dalla documentazione in atti non risulta l'inserimento della password. Con riferimento alla fase di accesso, si osserva che, se l'utilizzo del dispositivo oggetto di *enrollment* rappresenterebbe un elemento di possesso (ma restano i problemi in merito alla prova della SCA per l'*enrollment*), i log non contengono specifica evidenza dell'inserimento della password e del PIN, che rappresenterebbero elementi di conoscenza.
Con riferimento ai bonifici, va rilevato che l'utilizzo del dispositivo oggetto di *enrollment* potrebbe anche qui rappresentare un elemento di possesso, sebbene non vi sia specifica evidenza della push. Quanto all'elemento di conoscenza, l'inserimento del PIN, quale elemento necessario dell'autenticazione, viene menzionato solo nella legenda esplicativa dei log.
Alla luce della precedente ricostruzione dei fatti, considerata l'assoluta rilevanza che nell'impianto della disciplina dettata dalla Direttiva PSD2 assume l'elemento della doppia autenticazione, rilevato che anche da tale considerazione deriva la necessità di un rigoroso assolvimento da parte dell'intermediario dell'onere su di lui gravante di provare la sussistenza in ogni caso concreto di tale elemento, onere che non appare peraltro sproporzionato, considerato che l' intera fase di autenticazione si colloca nell'ambito di controllo (e di conseguente "vicinanza alla prova") dell'intermediario stesso, il Collegio ritiene che nella specie non sia stata fornita prova sufficientemente certa della sussistenza della c.d. SCA.
Va allora ricordato che in presenza di mancanza anche parziale della prova di autenticazione, i Collegi sono unanimi nel ritenere che in tali casi il ricorso debba essere accolto integralmente, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova di colpa grave dell'utente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso nei confronti del primo intermediario e dispone che il medesimo corrisponda alla parte ricorrente la somma di € 14.970,00 con buona valuta; non accoglie il ricorso nei confronti del secondo intermediario.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario soccombente 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
FLAVIO LAPERTOSA