Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) SCIUTO	Membro designato dalla Banca d'Italia
(RM) PAGLIETTI	Membro designato dalla Banca d'Italia
(RM) GRANATA	Membro di designazione rappresentativa degli intermediari
(RM) MOSCO	Membro di designazione rappresentativa dei clienti

Relatore GIAN DOMENICO MOSCO

Seduta del 11/12/2020

FATTO

La società ricorrente disconosce l'esecuzione di un'operazione di bonifico effettuato sul portale *home banking* gestito dall'intermediario affermando la responsabilità dell'intermediario convenuto in relazione a un bonifico di 40.000,00 € disposto il 28 novembre 2019, alle ore 9.06, dal suo rappresentante tramite Corporate Banking Interbancario (in seguito, CBI) accreditato sul conto di un diverso beneficiario.

In particolare, in un primo momento la ricorrente predisponeva, dal portale *home banking* dell'intermediario, un bonifico dal proprio c/c n. **69 tenuto presso filiale della banca attiva che doveva essere in favore di un proprio conto (n.***71) presso la filiale di Perugia dell'intermediario convenuto, come quello oggetto della presente controversia. Dopo quasi un'ora, un dipendente dell'intermediario informava la ricorrente di aver annullato l'operazione in quanto era stato erroneamente indicato come conto di addebito e di accredito il medesimo conto corrente tenuto presso la resistente (c/c n.***71). La ricorrente comunicava dunque che avrebbe ripetuto il bonifico, questa volta immettendo le corrette coordinate, e, in un secondo momento, vi ha dunque proceduto, inserendo il "flusso", stampando poi la distinta dalla quale non emergevano anomalie, inserendo infine il PIN e il codice OTP. Afferma però di non aver ricevuto alcun avviso dell'esecuzione dell'operazione. Il giorno successivo informava l'intermediario del bonifico effettuato e del rilevato addebito nel c/c n. **69. Il 4 dicembre 2019, su

sollecitazione del ricorrente, l'intermediario accertava che il bonifico in questione era stato dirottato al conto di un altro cliente dell'intermediario, sconosciuto alla ricorrente. Seguendo le indicazioni fornite dall'intermediario, che tra l'altro qualificava l'evento come "*phishing*", denunciava il fatto alla Polizia Postale. Oltre alla debolezza del sistema di sicurezza informatica, la ricorrente lamenta anche che l'intermediario, pur avvertito dell'esecuzione del bonifico, non si è accorto del mancato accredito dell'importo.

La ricorrente rileva di aver fatto esaminare il computer da cui è stata predisposta l'operazione (in seguito, anche il PC) da un consulente tecnico, che confermava l'adeguatezza del sistema operativo e dei sistemi di sicurezza presenti sul computer stesso ai parametri richiesti dall'intermediario. L'analisi informatica ha evidenziato la presenza di file riconducibili a una frode bancaria, in grado di interporsi nel corso dello svolgimento dell'operazione tra chi effettua il bonifico e la banca, modificando il beneficiario e l'importo del flusso disposto, senza però alterare il codice OTP generato dal Token in possesso esclusivo del cliente.

La ricorrente esperiva dunque reclamo il 7 dicembre 2019, il quale è stato rigettato dall'intermediario con riscontro del 16 dicembre.

La ricorrente chiede pertanto che il Collegio "riconosca l'adempimento del cliente agli obblighi di cui all'Art. 7 d.lgs 11/2010, nonché l'assenza di dolo o colpa grave nella condotta da Egli tenuta in relazione all'intrusione informatica subita" e il diritto al rimborso "di € 40.000, corrispondente all'importo dell'operazione di pagamento contestata, oltre alla commissione di € 0,70 addebitata dalla Banca passiva per l'esecuzione dell'operazione e agli interessi legali dalla data di originario addebito".

L'intermediario resistente controdeduce affermando tra l'altro quanto segue. L'operazione di pagamento è stata autenticata, registrata e contabilizzata correttamente e non ha subito alcun malfunzionamento delle procedure necessarie per la sua esecuzione o altri inconvenienti allo stesso imputabili. Assicura che per usufruire del servizio di *home banking* è necessaria un'autenticazione "forte" che garantisce la sicurezza delle operazioni. Desume che la presenza di un *virus* sul PC attestato dalla relazione tecnica dalla stessa prodotta esclude di per sé la propria responsabilità per l'operazione disconosciuta. In assenza di particolari anomalie, si presume che ci sia stata una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento. Infine, secondo l'intermediario, stante il tempo trascorso tra la predisposizione del bonifico e la segnalazione, era impossibile, pur attivandosi tempestivamente, come avvenuto, recuperare la somma.

L'intermediario chiede pertanto al Collegio di rigettare il ricorso.

Parte ricorrente replica, tra l'alto, asserendo che non sono stati provati i *log* ufficiali, in quanto il documento prodotto a tal fine dall'intermediario non possiede le caratteristiche di inalterabilità necessarie a costituire un effettivo supporto probatorio; inoltre lo stesso non indica l'IP e nessun dato inerente al terminale che ha eseguito l'operazione, come il browser utilizzato o il sistema operativo. Non può pertanto dirsi assolto l'onere probatorio dell'intermediario.

La ricorrente contesta infine che l'attivazione di un sistema di *sms alert* avrebbe certamente permesso di revocare rapidamente l'ordine di pagamento.

L'intermediario controreplica che i *log* esibiti rappresentano piena prova delle operazioni effettuate e che la domanda della ricorrente riguardo alla documentazione completa è inammissibile in quanto se fosse offerta configurerebbe un illecito. Inoltre, la perizia presentata da controparte identifica anche il modus dell'installazione del *malware*, ovvero una pec inviata da un soggetto non identificato e aperta colpevolmente

e senza alcuna precauzione dalla ricorrente. Il ritardo nella gestione della frode è altresì, secondo l'intermediario, da ascriversi alla colpa grave della ricorrente.

L'intermediario conclude affermando che la contestata assenza del servizio di *sms alert* è da imputarsi alla ricorrente in quanto non ne ha mai richiesto l'attivazione. Servizio che in ogni caso non avrebbe impedito l'asserita frode.

In risposta alla memoria di replica dell'intermediario la ricorrente precisa ancora che l'esibizione dei *log*s ufficiali avrebbe certificato la postazione utilizzata per l'esecuzione dell'operazione e le informazioni relative all'ambiente di lavoro. Il regolamento UE 2016/679 obbliga l'intermediario a fornire i dati in questione in presenza di un interesse legittimo del richiedente.

L'intermediario replica infine che fornire i *log* richiesti sarebbe inutile dal momento che le credenziali in uso dal cliente possono essere utilizzate da qualsiasi dispositivo e postazione. Asserisce infine che, tenuto conto dell'inefficacia dell'*antivirus* presente sul PC, la ricorrente avrebbe dovuto rifarsi sul fornitore IT del *software* dell'*antivirus* e non contro la banca.

DIRITTO

1. I fatti concernenti l'avvenuta perpetrazione dell'operazione informatica fraudolenta ai danni della ricorrente non sono in contestazione.

La società ricorrente fruisce del servizio predisposto dall'intermediario sulla sua *home banking* di *Corporate Banking* Interbancario, c.d. CBI, che consente al cliente non consumatore che detenga conti correnti in una o più banche (cc.dd. "banche passive") di concludere un contratto con un'altra banca (c.d. "banca attiva") di modo che, accedendo al servizio bancario tramite il portale della sola banca attiva, questi possa effettuare operazioni sui propri conti presso gli altri intermediari passivi.

Nel caso di specie, parte ricorrente non disconosce di aver effettuato l'operazione di bonifico tramite il servizio CBI, ma lamenta che l'operazione stessa sia stata "dirottata" e accreditata su un c/c avente IBAN e intestatario differente rispetto a quello correttamente immesso nell'ordine di pagamento.

In sintesi la ricorrente, dopo aver regolarmente avuto accesso al sito di *home banking* gestito dall'intermediario, ha disposto un ordine di bonifico nei confronti di un suo c/c identificato con un codice IBAN che pur essendo stato digitato correttamente non è risultato essere quello dell'effettivo beneficiario del bonifico, un soggetto diverso e sconosciuto.

Non sono in discussione le modalità attraverso le quali è avvenuto l'accesso della ricorrente all'*home banking* ed è altresì incontestato che la truffa sia stata causata da un *virus* presente sul computer con il quale è stata effettuata l'operazione contestata (in seguito, anche il PC o il Computer).

Sulla base della perizia prodotta dalla ricorrente, la truffa sembra essere avvenuta a causa di un *malware* denominato Sload presente sul PC che "viene veicolato principalmente attraverso e-mail PEC fraudolente contenenti false fatture".

È dunque presumibile che la truffa sia stata realizzata attraverso l'impiego di *software* malevoli inseriti nel Computer, in grado di sovrascrivere i dati inseriti nella pagina web dell'*home banking* senza che la ricorrente possa averne avuto l'immediata percezione (fattispecie del c.d. *man in the browser o man in the middle*).

Quanto sopra risulta avvalorato sia dalla circostanza che il numero di Iban considerato corretto è del tutto differente rispetto a quello riferibile al conto presso il quale è stato accreditata la somma bonificata, il che sembra escludere la possibilità di

errori di digitazione di qualche lettera o numero dell'Iban da parte della ricorrente; sia dal fatto che non emergeva alcuna anomalia dalla distinta del flusso di pagamento che autorizzava a eseguire le operazioni in esso contenute. La ricorrente non poteva dunque rendersi conto della contestuale fraudolenta alterazione dei dati causata dal *malware*.

Così ricostruiti i fatti rilevanti, in diritto si tratta di stabilire se la responsabilità giuridica dell'accadimento sia imputabile all'intermediario.

2. Nel valutare il comportamento dell'intermediario alla luce del principio della c.d. diligenza professionale desumibile dall'art. 1176, comma 2, c.c., va osservato che con particolare riferimento all'attività bancaria e finanziaria, anche tenuto conto dei rilevanti interessi, sia individuali sia generali, a essa sottesi, il principio generale della responsabilità professionale ha trovato una particolare specificazione, tra l'altro, con riguardo all'utilizzazione di servizi e strumenti con funzione di pagamento che si avvalgono di mezzi elettronici nell'ambito della disciplina del d. lgs 27 gennaio 2010, n. 11, attuativo della direttiva 2007/64/Ce relativa ai servizi di pagamento nel mercato interno, la quale prevede una serie di obblighi e oneri, anche sotto il profilo della ripartizione della prova in caso di operazioni non autorizzate, a carico tanto dell'intermediario, quanto dell'utilizzatore dei servizi di pagamento.

È stato pertanto riconosciuto il principio secondo il quale la possibilità di comportamenti fraudolenti nell'effettuazione di operazioni di pagamento attraverso strumenti di pagamento, purché non riconducibile a frode, dolo o colpa grave dell'utente, va ricondotta all'area di rischio professionale dei prestatori dei servizi di pagamento (v. i principi espressi in Cass. n. 2950/2017; v. anche Cass. 5 luglio 2019, n. 18045; v. la decisione del Collegio di coordinamento n. 3498/2012).

Per quanto qui più rileva, l'art. 10 del d. lgs n. 11/2010 dispone che "qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente 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" (comma 1). Con la precisazione 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 (…) 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", compreso tra l'altro quello di "utilizzare lo strumento di pagamento in conformità con i termini" contrattuali "che ne regolano l'emissione e l'uso" (art. 7, comma 1 lett. a), essendo in ogni caso "onere del prestatore di servizi di pagamento (…) fornire la prova della frode, del dolo o della colpa grave dell'utente" (comma 2).

Nel caso di specie, l'intermediario ha fornito la prova che "l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata". Nondimeno, non è riuscito a dimostrare che l'operazione contestata "non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti".

Al contrario, l'intermediario ha riconosciuto che la ricorrente possa essere stata vittima della truffa informatica. Tuttavia, imputa a quest'ultima l'esclusiva responsabilità dell'accaduto in quanto la ricorrente ha l'obbligo accedere ai Servizi attraverso un computer dotato di idonei requisiti di sicurezza volti a prevenire azioni fraudolente e furti

di identità elettronica. Ciò solo per il fatto che la stessa ricorrente ha ammesso che il suo Computer è stato infettato da un *malware*, dimostrando dunque di essere stata poco accorta nella sua protezione.

La deduzione dell'intermediario è priva di fondamento.

La norma contrattuale sopra riportata va infatti interpretata alla luce della sopra richiamata previsione dell'art. 10, comma 2, d. lgs n. 11/2010 secondo la quale è onere dell'intermediario "fornire la prova della frode, del dolo o della colpa grave dell'utente", senza che ciò possa essere presunto dal mero fatto dell'utilizzo "di uno strumento di pagamento registrato dal prestatore di servizi di pagamento".

Questo principio applicato al caso di specie implica che alla ricorrente non può essere imputata alcuna colpa grave per il solo fatto che l'operazione fraudolenta sia stata comunque realizzata nonostante il regolare accesso al servizio di *home banking*. Conseguentemente, non è neppure consentito far risalire la sua colpa grave a una mancata protezione adeguata del PC.

Ciò anche senza considerare che la frode informatica oggetto del ricorso è valutata tra le più sofisticate e insidiose, tanto da riuscire a eludere gli stessi protocolli di controllo predisposti degli intermediari.

4. Del resto, l'intermediario riconosce la mancata attivazione del servizio di *sms alert*.

Il Collegio di Coordinamento con decisione n. 16237 del 26 luglio 2018 ha ribadito che il servizio "*sms alert*" costituisce ormai uno standard di sicurezza normalmente esigibile in relazione all'utilizzo delle carte di pagamento e, dunque, un presidio di sicurezza divenuto ormai necessario per la tutela degli utilizzatori di tali strumenti. La mancanza di questo servizio è dunque di per sé idonea a spostare verso l'intermediario il rischio connesso a operazioni fraudolente avvenute con l'impiego di tali strumenti, costituendo una disfunzione organizzativa a lui imputabile (v. decisione n. 12441/2019 del Collegio di Roma).

Nel caso di specie, è pacifico che il servizio di allerta automatico non sia stato predisposto e (o) attivato dall'intermediario, non consentendo così la presa di coscienza da parte della ricorrente delle operazioni illecite.

5. Alla luce di quanto sopra, l'intermediario va considerato giuridicamente responsabile delle conseguenze dannose subìte dalla ricorrente per i fatti controversi.

Il ricorso va dunque accolto limitatamente al diritto di parte ricorrente a ricevere la somma sottratta in seguito all'attacco del *malware* presente nel suo Computer con i relativi interessi legali.

P.Q.M.

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 40.000,00 oltre agli interessi legali dalla richiesta al saldo. Respinge nel resto.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA