Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) BERTI ARNOALDI VELI	Membro designato dalla Banca d'Italia
(BO) LONGOBUCCO	Membro designato dalla Banca d'Italia
(BO) LUCARELLI	Membro di designazione rappresentativa degli intermediari
(BO) SARZANA DI S. IPPOLITO	Membro di designazione rappresentativa dei clienti

Relatore CATERINA LUCARELLI

Seduta del 19/06/2018

FATTO

Titolare del rapporto di conto corrente X aperto presso l'intermediario convenuto al quale è associata la carta di pagamento Y ed un servizio di home banking, la parte ricorrente, anche a mezzo della documentazione acclusa al ricorso, riferisce che in data 9.8.2017, dovendo effettuare alcune operazioni tramite home banking, accedeva, come al solito, al sito internet dell'intermediario, seguendo l'apposito link memorizzato nella sezione "Preferiti" del proprio browser. Dunque, si collegava ad una schermata internet, che presentava gli stessi caratteri e colori del sito dell'intermediario, contenente, altresì, il logo dello stesso, in cui le veniva richiesto l'inserimento di una password dispositiva a conferma della propria identità, inseriva, dunque, la carta di pagamento in propria titolarità all'interno dell'apposito lettore in sua dotazione che generava, conseguentemente, un codice che provvedeva ad inserire on line; una volta terminata questa operazione le veniva negato l'accesso al conto on line. Lo stesso giorno, nel pomeriggio, dopo aver tentato un nuovo accesso alla propria area personale, che le viene interdetto, chiamava il call center dell'intermediario e veniva informata del fatto che alle ore 10,37 del 9.08.2017 era stato effettuato, con addebito sul conto corrente X, un bonifico dell'importo di euro 12.848,00. Chiesto immediatamente il blocco del bonifico in quanto dalla stessa non autorizzato né

eseguito, sporta denuncia per l'accaduto, presentato reclamo all'intermediario per ottenere il rimborso del bonifico disconosciuto, che resta riscontrato negativamente, la parte inoltra ricorso all'Arbitro Bancario e Finanziario per la immediata rifusione della somma di euro 12.848,00 perché non autorizzata.

Convenuto ritualmente, l'intermediario precisa che il codice autorizzativo inserito dalla ricorrente è generato da un apposito lettore PCR rilasciato ai fini utilizzativi dell'home banking, ovvero un dispositivo che permette la generazione e lo scambio di codici univoci tra il sito web e il correntista. L'intermediario precisa che la digitazione del codice autorizzativo di ciascuna transazione viene richiesto esclusivamente dopo che il cliente abbia scelto il tipo di operazione da effettuare, mentre nel caso di specie la ricorrente non aveva ancora effettuato tale scelta. Il giorno successivo all'esecuzione del bonifico, ossia il 10.08.2017, è stata avanzata alla banca del beneficiario del bonifico una richiesta di recall dello stesso, finalizzata al recupero della somma dalla giacenza presente sul conto corrente di destinazione della transazione, ma non è stata ottenuta alcuna risposta, presumibilmente a causa del fatto che la banca beneficiaria non ha trovato un deposito sufficiente sul conto corrente del beneficiario dell'operazione di pagamento. Per queste ragioni, e per le connesse ragioni di diritto, l'intermediario chiede all'Arbitro Bancario e Finanziario, di rigettare il ricorso in oggetto.

DIRITTO

ABF ha più volte affermato che nelle controversie relative ad un utilizzo fraudolento di strumenti di pagamento, occorre valutare, da un lato, la condotta dei clienti con riguardo agli obblighi di diligenza nella custodia dello strumento di pagamento e dei dispositivi collegati, dall'altro, la condotta dell'intermediario, il quale è chiamato ad adempiere al mandato secondo la diligenza professionale e qualificata dell'art. 1176, comma 2, c.c., attraverso l'adozione di misure di protezione adeguate rispetto agli standard esistenti, sotto il profilo dei presidi tecnici adottati.

L'orientamento dei Collegi ABF è nel senso di ravvisare la colpa grave del cliente per imprudente navigazione qualora risulti che quest'ultimo abbia comunicato a terzi i dati associati ad uno strumento di pagamento in risposta ad una e-mail di phishing ovvero SMS.

Sono ormai molteplici, infatti, le modalità attraverso le quali vengono perpetrate le frodi attraverso internet (invio di mail-civetta volte ad indurre i clienti a comunicare i propri dati personali, malware di reindirizzamento web, ecc.).

In materia assumono particolare rilevanza le decisioni n. 3498/2012 e n. 1820/2013, con le quali il Collegio di coordinamento ha distinto le truffe realizzate mediante metodi ormai conosciuti alla clientela (le classiche email di phishing), dalle truffe più insidiose in cui maggiore è la difficoltà di avvedersi della situazione di apparenza generata dal malware.

In particolare, il Collegio di Coordinamento con le suddette decisioni, ha distinto le ipotesi di "phishing tradizionale", caratterizzate dall'invio di un semplice messaggio telefonico o e-mail con il quale si invita il cliente a digitare le proprie credenziali di accesso al conto, da quelle più insidiose consistenti in un "subdolo meccanismo di aggressione (che) ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino".

Tra le due fattispecie v'è una differenza tale da indurre a ritenere che solo nella seconda, consistente in una sofisticata intrusione nell'autentico sito della banca nel momento in cui l'utente vi accede per compiere un'operazione, debba escludersi la ravvisabilità di una colpa grave del cliente; laddove nel caso di phishing tradizionale, l'assenza di cautela dell'utente appare difficilmente scusabile, trattandosi in tal caso di fenomeno oramai diffusamente noto, che quanto meno qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso del c.d. homebanking, deve essere in grado di individuare, non facendosi trarre in inganno.

La parte ricorrente disconosce un bonifico on line dell'importo di 12.848,00 euro effettuato in data 9.08.2017 con addebito sul rapporto di conto corrente X. La ricorrente dichiara di aver effettuato l'accesso al sito internet dell'intermediario seguendo l'apposito link memorizzato nella sezione "Preferiti" del proprio browser, collegandosi ad una schermata internet che presentava gli stessi caratteri e colori del sito dell'intermediario, contenente, altresì, il logo dello stesso, in cui però le veniva richiesto l'inserimento di una password dispositiva a conferma della propria identità. La ricorrente ha assecondato questa richiesta, inserendo la carta di pagamento in propria titolarità all'interno del lettore in sua dotazione che ha generato, conseguentemente, un codice che la ricorrente ha inserito on line.

Nel caso in esame, appare incontestato che l'intermediario abbia adottato un sistema di sicurezza "a due fattori", ossia l'operazione contestata, ovvero il bonifico on line dell'importo di 848,00 euro, è avvenuta non solo mediante la digitazione delle credenziali previste, ma anche attraverso l'utilizzo fisico di un dispositivo PCR che, insieme alla carta, permetteva, al momento dell'effettuazione della transazione on line, la generazione e lo scambio di codici univoci tra il sito web e il correntista. Rilevante è il fatto che sia stata richiesta alla ricorrente la digitazione della password OTP "dispositiva", ovvero necessaria ad autorizzare le operazioni di pagamento, al momento del login all'interno del sito dell'intermediario; questa circostanza, avrebbe dovuto indurre in sospetto la ricorrente. Mentre non rilevante risulta la mancata produzione dei log dell'operazione contestata, da parte dell'intermediario, in quanto per ammissione della stessa ricorrente, è stata proprio lei ad inserire le credenziali e la password generata dal dispositivo PCR in suo possesso.

Appare, pertanto, pacifico che l'operazione contestata sia scaturita da un fenomeno di frode attraverso internet realizzato ai danni della cliente, avendo la stessa ricorrente fornito tutti i dati necessari per l'esecuzione dell'operazione oggi contestata, in una fase (l'accesso al sito) in cui non vengono richieste password dispositive. Ne consegue che la colpa grave della ricorrente risulta provata, essendo indubitabile che l'operazione abusiva contestata è stata resa possibile dal suo comportamento. E tale comportamento denuncia una colpevole violazione degli obblighi di custodia dei dati identificativi e dispositivi del proprio conto.

Tali circostanze, secondo il consolidato orientamento in materia (v., tra le altre, Collegio di coordinamento, decisione n. 3498/2012; Collegio di Milano, decisione n. 467/2014 e Collegio di Roma, n. 1699/2013), non possono che indurre a ribadire che al ricorrente è imputabile una violazione gravemente colpevole degli obblighi di custodia dei dati identificativi e dispositivi del conto on line, sicché la perdita subita non può che restare interamente a proprio carico, in linea con il costante orientamento ABF(ex multis, Collegio di Bologna, decisione n. 6803/18; Collegio di Bologna, decisione n. 4585/18; Collegio di Napoli, decisione n. 7483/17; Collegio di Milano, decisione n. 9731/17). Pertanto, il ricorso non può trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI