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) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) DENOZZA

Seduta del 23/09/2024

FATTO

La cliente espone:

- In data 7 dicembre 2023, veniva disposto, in uscita dal proprio conto corrente, un bonifico istantaneo del valore di € 14.950,00 su un conto corrente estero, con causale “giroconto”;
- ha provveduto a disconoscere l’operazione fraudolenta in data 14/12/2023;
- in quella data non ha mai ricevuto alcuna telefonata, SMS alert o notifica Push;
- il beneficiario del bonifico sembrerebbe avere il medesimo cognome della cliente, ma non ne si conosce il nome di battesimo;
- ha subito una frode informatica che ha comportato il furto della sua identità, questa frode ha permesso all’autore di aprire un conto corrente intestato all’estero a suo nome e di effettuare un bonifico, tutto ciò è stato possibile a causa delle carenze nella sicurezza dei sistemi dell’intermediario;
- non ha mai fornito i propri dati di accesso al conto corrente a nessuno;
- il suo telefono non è stato clonato, per di più non hai mai conservato nel proprio telefono copie dei propri documenti, necessari per poter aprire un conto corrente;
- esponeva reclamo in data 11/12/2023, al quale l’intermediario rispondeva negativamente affermando che non si è presentato alcun malfunzionamento, l’operazione è stata registrata e contabilizzata correttamente;

- ha fornito prova che in quel giorno non ha fatto uso del traffico dati dal proprio device mobile;
- ha provato a raggiungere un accordo anche tramite difensore legale, ma l'intermediario non si rendeva disponibile a trovare un accordo.

Chiede la restituzione di € 14.950, 00 almeno in parte.

L'intermediario afferma:

- la ricorrente è titolare del conto corrente n.***870 (a lei intestato) al quale è collegato il servizio "Rapporti a distanza tra Banca e Cliente", c.d. home banking che consente ai clienti di effettuare le operazioni di inquiry e dispositive sui conti correnti personali a loro riferibili, utilizzando il telefono cellulare o Internet;
- la ricostruzione degli accadimenti riportata in denuncia non permette di apprendere le modalità di svolgimento della frode;
- in data 27/11/2023 alle ore 15:07 (molti giorni prima della frode), la banca ha inviato al numero di cellulare della cliente il messaggio di attivazione del (secondo) Mobile Token; pertanto, se tale operazione non fosse stata da lei richiesta, avrebbe dovuto insospettirsi, e contattare subito l'assistenza;
- precisa che il Mobile Token non può essere attivato in alcun modo, senza l'utilizzo dei codici di sicurezza, conosciuti solo dal titolare dei canali diretti;
- in presenza di un sistema in astratto valutabile come sicuro, come quello adottato dalla banca e in assenza di particolari anomalie di sistema, si deve presumere che ci sia stata una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento;
- il comportamento tenuto dalla ricorrente, che ha permesso l'attivazione del (secondo) Mobile Token, conferma la sua colpa grave, per non avere adempiuto con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate del proprio strumento di pagamento, nonostante il messaggio pervenuto sul suo cellulare che la informava dell'esecuzione di un'operazione dalla stessa non richiesta (attivazione secondo Mobile Token);
- anzi, la cliente ha ricevuto il messaggio per l'attivazione del (secondo) Mobile Token (27/11/2023) con l'OTP relativo e non lo ha tenuto per sé, contravvenendo alla raccomandazione di assoluta riservatezza del dato contenuta nel messaggio;
- è evidente, infatti, che la ricorrente abbia "abboccato" ad un messaggio e/o a una telefonata di phishing, che rappresenta un tipo di frode considerato conosciuto come strumento di approfittamento della credulità dei malcapitati, quindi inescusabile e ritenuta elemento qualificabile come colpa grave da parte dei Collegi ABF;
- a fronte delle operazioni eseguite, la banca ha inoltrato i messaggi SMS e le relative notifiche push,
- la banca, una volta allertata dell'avvenuta frode, ha subito esperito il tentativo di recupero (tardivo), presso la banca corrispondente, della somma oggetto di frode, ricevendo esito negativo.

Chiede la reiezione del ricorso.

DIRITTO

L'operazione contestata, di importo pari a € 14.950,00 è stata effettuata il 07/12/2023 alle ore 16:18. Trattasi di un bonifico online a debito del conto corrente. È in atti la denuncia presentata dalla ricorrente, in data 11/12/2023. Nella denuncia la cliente descrive la truffa

nei medesimi termini del ricorso. Afferma in particolare, di non avere mai ceduto a terzi i codici di accesso all'home banking né i codici di pagamento.
Circa le modalità di esecuzione delle operazioni in questione l'intermediario rileva che il conto corrente cointestato al cliente è collegato al servizio "*Rapporti a distanza tra Banca e Cliente*", c.d. *home banking*. Tale servizio di *home banking* prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte" che in caso di accesso tramite *App* prevede, per effettuare il *login e* funzioni di *inquiry*, l'inserimento delle credenziali di sicurezza (numero cliente + PIN) + codice OTP, generato da *Mobile Token* e per disporre le operazioni, dopo aver effettuato il *login* ed inserita l'operazione, la conferma mediante inserimento del PIN + codice OTP generato da *Mobile Token*.
Il codice OTP è generato in modo silente da *Mobile Token* integrato nella *App* che il cliente ha attivato sul proprio *device*. La cliente può attivare il *Mobile Token*, contemporaneamente su due dispositivi (2 *smartphone* oppure 1 *smartphone* + 1 *tablet*) ed inoltre è libera di sostituire il proprio *device* senza dover comunicare il nuovo modello alla banca se il numero di cellulare resta invariato. L'attivazione del *Mobile Token* avviene tramite autenticazione "forte", infatti, essa è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via email e via sms, indipendentemente dalla attivazione del servizio sms *Alert*.
Fatte queste premesse, l 'intermediario con riferimento al login e all'attivazione di un nuovo mobile token, produce evidenza da cui è possibile ricavare che in data 27/11/2023 alle ore 11:01 è stata autorizzata una transazione internet tramite Strong Customer Authentication con PIN ed OTP transazionale silente (vd. colonna OTP popolata e relativa legenda esplicativa) e che alle ore 15:06 è stato eseguito un tentativo di accesso alla app tramite inserimento dell'ID utente e del pin con l'utilizzo di un device diverso da quello precedente.
Sempre in data 27/11/2023 alle ore 15:08:55 si procedeva all'attivazione del Mobile Token che, alle 15:08:55 risultava attivato. In merito a tale attivazione, si osserva che, secondo la ricostruzione dell'intermediario, la stessa è stata resa possibile dall'inserimento di un OTP ricevuto via sms, e che in effetti la corrispondente colonna OTP risulta popolata. Mentre risulta provato l'invio del codice OTP (elemento di possesso), non risulta invece prova certa della presenza del secondo fattore.
Quanto al login prodromico all'operazione di bonifico posta in essere, l'intermediario produce evidenza da cui si ricava che alle ore ora 16:18:29 07/12/2023 è stato eseguito l'accesso all'home banking. Alla luce della legenda si rileva che l'inserimento dell'ID Utente risulta dalla relativa colonna popolata mentre la generazione dell'OTP silente risulta dalla relativa colonna popolata.
Non si ha però diretta evidenza dell'inserimento del PIN. Non è infatti presente specifica evidenza dell'inserimento del PIN, il cui utilizzo risulta solo dalla descrizione attività utente. La colonna esito operazione non è in alcun modo valorizzata.
Con riferimento infine alla transazione contestata, sulla base delle evidenze prodotte è possibile osservare che non si rinviene nella documentazione in atti evidenza della notifica push e non si ha diretta evidenza dell'utilizzo del PIN se non nel campo attività. Trattandosi di un'operazione autenticata nell'ambito della sessione precedentemente aperta, potrebbe teoricamente ammettersi il "riutilizzo" di uno dei fattori di autenticazione precedentemente impiegati per l'apertura della sessione. Nel caso di specie vanno tuttavia, richiamate le riserve sopra esposte con riferimento al login.
Sulla base di quanto precede, 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 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 e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 14.950,00.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA