COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) GRIPPO

Seduta del 25/05/2023

FATTO

Parte ricorrente afferma che: suo marito, delegato ad operare sul proprio conto corrente, in data 23/09/2022 riceveva un SMS apparentemente proveniente dall'intermediario convenuto in quanto collocato nella chat genuina e preceduto da messaggi autentici; il marito quindi cliccava sul link contenuto nell'SMS e ricevuta una successiva telefonata, seguiva le istruzioni del sedicente operatore; durante la telefonata non sono stati mai comunicati codici segreti; si accorgeva di essere stata vittima di una truffa in quanto riscontrava bonifici non autorizzati; in ogni caso, le operazioni contestate superano i massimali giornalieri pattuiti.
Parte ricorrente – esperita senza successo la fase del reclamo – chiede il rimborso della somma di € 64.989,88.
L'intermediario, con le controdeduzioni, precisa che: parte ricorrente è stata vittima di smishing misto a vishing; la ricostruzione offerta dalla cliente è lacunosa; in ogni caso, l'ammontare complessivo delle operazioni contestate è pari a € 64.979,98 (commissioni incluse) e non pari a € 64.989,88 come indicato nel ricorso; le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto risulta che le operazioni sono avvenute con il corretto inserimento delle credenziali; sussiste la colpa grave della cliente che ha ceduto il controllo del proprio conto e dei dispositivi collegati all'ex marito il

quale, a sua volta, ha ceduto le credenziali e comunicato i codici al truffatore; non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.
L'intermediario chiede, pertanto, di rigettare il ricorso perché infondato.
Parte ricorrente, in sede di repliche, afferma che: l'SMS truffaldino non presentava errori ortografici o di sintassi; l'intermediario non ha fornito prova dell'autenticazione forte, in particolare per l'innalzamento dei massimali; non è stato ricevuto alcun SMS alert; il numero e l'importo delle operazioni presentavano caratteri di anomalia che i sistemi della banca avrebbero dovuto intercettare.
L'intermediario, in sede di controrepliche, precisa che: l'SMS ricevuto non è collocato nella chat ufficiale con la banca e presenta caratteri di anomalia; il LINK ivi presente non è riconducibile alla banca; la colpa grave della cliente sussiste per avere ceduto il proprio strumento di pagamento ad un terzo, il proprio ex coniuge; peraltro, la APP risulta associata al device dell'ex coniuge sin dall'apertura del rapporto; è stata comunque fornita la prova della corretta autenticazione.

DIRITTO

La controversia sottoposta all'esame del Collegio verte sulla ormai nota questione del furto di strumenti di pagamento e sul rimborso di somme indebitamente sottratte a seguito di disposizioni fraudolentemente impartite.
Le operazioni contestate da parte ricorrente (n. 18 operazioni di cui 7 bonifici e 11 pagamenti con carta di debito per un importo complessivo di € 64.979,98, tutte effettuate in data 23/9/2022 tra le ore 9.39 e le ore 11.17) rientrano nell'ambito di applicazione della disciplina del D. Lgs. 27/1/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
La normativa richiamata ha provveduto a ripartire una serie di obblighi tra il prestatore di servizi di pagamento e l'utilizzatore di detti servizi. L'utilizzatore, in particolare, ha il dovere di utilizzare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici PIN). Per quanto riguarda l'intermediario, la normativa ricordata prevede, tra gli altri, l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi.
Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.
La normativa mostra un chiaro favor probatorio nei confronti dell'utilizzatore, in quanto l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo oppure che questi abbia agito in modo fraudolento ovvero con dolo o colpa grave.
La ratio di tale scelta legislativa è notoriamente quella di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento (Corte di Cassazione, sentenza n. 9158/2018).
Alla luce di tali disposizioni, pertanto, due sono i passaggi ineludibili in materia. In primo luogo è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova che comunque di per sé non è

sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
Con riferimento alla strong customer authentication (cd. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).
Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente: 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi, infine, devono essere reciprocamente indipendenti e appartenere a categorie diverse.
Nel caso in esame, trattasi di n. 11 operazioni di acquisto online con carta di pagamento e n. 7 operazioni di bonifico; tali operazioni sono state precedute dalle seguenti azioni preliminari poste in essere dal truffatore: 1) l'accesso al conto, 2) l'enrollment della APP su un nuovo dispositivo, 3) la modifica del PIN dispositivo, 4) la creazione di n. 4 carte di pagamento virtuali, 5) l'innalzamento dei massimali per ciascuna carta virtuale.
L'intermediario afferma che sia le azioni preliminari sia le singole operazioni di pagamento sono state eseguite tramite una procedura di autenticazione forte a doppio fattore.
Il Collegio rileva, invero, che dall'esame della documentazione prodotta l'intermediario non ha dato prova dell'autenticazione forte per le operazioni di enrollment del nuovo dispositivo (in particolare, contrariamente alla procedura specificata dallo stesso intermediario, a seguito dell'invio della e-mail contenente il link di conferma per convalidare l'associazione ad un nuovo dispositivo, non si rinviene evidenza dell'ulteriore codice OTP a 4 cifre inviato tramite SMS all'utenza mobile registrata) e per la modifica del PIN dispositivo (in particolare non viene specificato il processo di autenticazione forte previsto per tale modifica e non vi è prova del sistema di autenticazione a doppio fattore).
Il Collegio ricorda che è onere dell'intermediario provare che sia le operazioni preliminari sia le singole operazioni contestate siano state autenticate, correttamente registrate e contabilizzate.
In mancanza della suddetta prova l'intermediario sopporta –come nel caso di specie- integralmente le conseguenze delle operazioni disconosciute (cfr. Collegio di Milano, decisione n. 1588 del 17 febbraio 2017).
Per quanto esposto, questo Collegio dispone a favore di parte ricorrente il rimborso della somma di € 64.980,00, pari all'ammontare delle operazioni disconosciute.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 64.980,00.
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