Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) FERRANTE	Membro designato dalla Banca d'Italia
(TO) SETTEMBRE	Membro designato dalla Banca d'Italia
(TO) SPAGNOL	Membro di designazione rappresentativa degli intermediari
(TO) CATTALANO	Membro di designazione rappresentativa dei clienti

Relatore LUCA CATTALANO

Seduta del 21/02/2024

FATTO

Parte ricorrente, dopo aver inutilmente esperito reclamo in data 19.09.2023, riferiva le proprie ragioni di controversia che si possono così riepilogare:

- di essere titolare di un conto corrente, acceso presso la resistente;
- che in data 20/07/2023 verso le ore 19.35 riceveva dalla banca un sms con il quale veniva edotta della necessità di aggiornare il proprio servizio telematico bancario, venendo altresì avvisata dell'imminente telefonata da parte di un operatore;
- che tale messaggio perveniva attraverso il canale di messaggistica ufficiale della banca e da questa utilizzato per le ordinarie comunicazioni con la clientela;
- che alle 19.39 riceveva la telefonata preannunciata dal messaggio in occasione della quale il sedicente operatore – che era già a conoscenza della password di accesso all'home banking – le dettava la procedura da seguire per l'aggiornamento;
- che, espletata la procedura, visionava l'estratto conto, avvedendosi che ignoti aveva disposto due transazioni fraudolente per complessivi € 12.000,00;
- che quindi disponeva il blocco dello strumento di pagamento e sporgeva denuncia presso le autorità competenti;
- che disconosceva le operazioni e formulava reclamo alla banca, senza ottenere alcun rimborso;

- che tuttavia la banca non ha prodotto alcunché a sostegno della regolarità formale delle operazioni;
- che la banca ha violato il comma 1 dell'art. 8 del d.lgs 11/2010, non impedendo l'accessibilità al dispositivo a soggetti diversi dal soggetto legittimato ad usare lo strumento di pagamento;
- che nessuna "colpevole credulità" può esserLe ascritta dal momento che è stata vittima di una truffa insidiosa, essendo sia l'SMS civetta sia la telefonata provenuti da una utenza telefonica ufficiale riconducibile alla banca;
- che in tal senso verte la giurisprudenza dell'ABF.

Concludeva per ottenere il rimborso della somma complessivamente sottratta di € 12.000,00.

Nel costituirsi con controdeduzioni l'intermediario resistente, sosteneva le proprie ragione di opposizione alle avversarie domande richiamando l'attenzione sul fatto:

- che la truffa di c.d. *smishing* - di cui è rimasta vittima la ricorrente - è ampiamente nota;
- che la banca pertanto già da febbraio 2022 ha svolto una campagna informativa rivolta alla clientela circa le diverse tipologie di truffe, fornendo altresì indicazioni per evitarle;
- che il sistema di Home Banking adottato dalla Banca resistente prevede, altresì, la notifica in automatico di messaggi - in cui sono descritte dettagliatamente le richieste che il cliente non deve assecondare – dei quali il cliente deve necessariamente prendere visione per poter accedere alle funzioni della propria area riservata;
- che pertanto la banca ha messo la cliente nella condizione di riconoscere la truffa ordita dai malfattori ai suoi danni;
- che nel contratto, in particolare agli artt. 2 e 3, sono previsti precisi obblighi in uso in capo alla cliente di conoscenza della rete internet e dei sistemi impiegati;
- che i servizi di pagamento adottati dalla Banca sono conformi agli standard di sicurezza previsti dalla Regolamentazione europea in materia, prevedendo dunque un doppio fattore di autenticazione;
- che, in particolare, per accedere al Servizio di Internet Banking e disporre le operazioni, occorre inserire lo user ID, il PIN e il codice OTP (login/dispositivo), generato dal dispositivo X Pass Code;
- dall'analisi del tracciato dei log è possibile verificare che le operazioni effettuate in data 20/07/2023, sono state eseguite con il regolare inserimento dei codici autorizzativi di esclusiva pertinenza della cliente;
- che, all'esito delle verifiche effettuate sulla linea telefonica, il fornitore del servizio ha escluso la presenza di anomalie di natura tecnica sulla stessa;
- che la cliente che ha dato seguito alle istruzioni ricevute dal malfattore è incorsa in colpa grave;
- che le richieste ricevute dovevano indurre in sospetto la cliente laddove, nel primo sms, veniva chiesto di cliccare su di un link inesistente;
- che la cliente usando la normale diligenza, alla ricezione del primo sms, avrebbe dovuto contattare il Servizio Clienti della Banca deputato a fornire ogni chiarimento sui prodotti e i servizi resi dai sistemi di pagamento e avrebbe con ciò evitato di incorrere nella frode;
- che la colpa grave della ricorrente emerge altresì dalla circostanza che è avvenuta la disinstallazione della licenza del suo *device* e l'*enrollment* di un nuovo *device* grazie al codice inviato via email all'istante e da questa comunicato;

- che la giurisprudenza ordinaria ha escluso profili di responsabilità in capo alla Banca nel caso in cui la truffa è stata realizzata solo grazie alla condotta gravemente colpevole del cliente, senza la quale i malfattori non avrebbero potuto materialmente eseguire e portare a termine il bonifico disconosciuto.

Concludeva per il rigetto del ricorso.

Nelle repliche alle controdeduzioni, la parte ricorrente rilevava:

- che non è vero che è previsto il doppio fattore in fase e di accesso all'home banking, nonché ai fini dell'autenticazione delle singole operazioni di pagamento, in quanto lei inserisce solo ed esclusivamente il proprio codice utente e il proprio PIN, mentre nessuna password dinamica viene richiesta;
- che non sussiste alcuna sua colpa grave in quanto l'SMS truffaldino - dal quale ha preso origine la truffa e che ha sicuramente rappresentato una *condicio sine qua non* della medesima - le è pervenuto sulla chat ufficiale del PSP, in coda a precedenti messaggi autentici e genuini;
- che il messaggio civetta, inoltre, non contenendo alcun errore grammaticale e/o di sintassi, e recando all'interno del link la denominazione sociale del PSP, non poteva insospettirla;
- che anche la telefonata truffaldina che ha perfezionato la frode è pervenuta alla ricorrente attraverso un'utenza telefonica ufficiale ed effettivamente riconducibile all'intermediario resistente;
- che la "campagna pubblicitaria" di cui ha riferito la controparte, prima del 20/07/2023 (giorno nel quale è stata perpetrata la frode oggetto di controversia), non era affatto visibile sulle pagine web della banca;
- che, pertanto, nel caso di specie, non vi erano elementi che potessero indurla a dubitare dell'autenticità e della veridicità della comunicazione messaggistica e telefonica poi rivelatesi truffaldine.

Nelle repliche la parte ricorrente ha aggiunto in via subordinata la domanda di accertamento di un concorso di colpa tra le parti, con conseguente diritto alla restituzione del 50% dell'importo delle transazioni oggetto di controversia, per una somma pari a € 6.000,00

DIRITTO

Il presente ricorso riguarda nr. n. 2 bonifici, effettuati in data 20/07/2023 di cui uno di € 3.000,00 e uno di € 9.000,00.

Tali operazioni risultano dall'estratto conto, oltreché dalla denuncia

Tanto premesso in ordine alla tipologia della operazione contestata, va preliminarmente ricordato che il d.lgs. n. 11/2010 di recepimento della direttiva 2007/64/CE in materia di servizi di pagamento (meglio nota come PSD) ha ripartito gli obblighi del prestatore e dell'utilizzatore di tali servizi, da un lato, imponendo all'utilizzatore gli obblighi di utilizzare lo strumento di pagamento in conformità con il contratto stipulato con il prestatore (art. 7), di comunicare senza indugio al prestatore le operazioni di pagamento non autorizzate di cui sia venuto a conoscenza (art. 9) e di adottare accorgimenti idonei a garantire la sicurezza e la riservatezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento stesso (art. 12) e, dall'altro lato, imponendo al prestatore, tra gli altri, l'obbligo di adottare presidi di sicurezza atti ad "assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi posti in capo a quest'ultimo" (così l'art. 8, comma 1, lett. a), del citato d.lgs. n. 11/2010).

Un portato della normativa appena richiamata è che, qualora l'utilizzatore neghi di aver autorizzato un'operazione di pagamento, grava sull'intermediario provare che l'operazione stessa è stata autenticata, correttamente registrata, contabilizzata, e che durante la sua esecuzione non si siano verificati malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10). Nel caso di mancato assolvimento, in tutto o in parte, di detto onere probatorio gravante sull'intermediario, la richiamata disciplina prevede che l'intermediario sopporti la relativa perdita, atteso il fatto che quest'ultimo si è assunto il rischio d'impresa connesso con l'esercizio dell'attività ed è in grado di ribaltare tale rischio sulla massa degli utenti attraverso la determinazione dei prezzi per la fornitura del servizio (cfr. Collegio di Roma, decisione n. 1111/2010, richiamata dalla decisione del Collegio di Coordinamento n. 3498/2012).
Quanto precede trova un limite nella circostanza che l'utilizzatore abbia agito mancando di osservare in modo fraudolento o gravemente colposo i richiamati obblighi di corretto utilizzo e di custodia degli strumenti di pagamento, situazione nella quale l'art. 12, comma 4, del d.lgs. n. 11/2010, prevede che l'utilizzatore sopporti per intero le perdite subite.
Si deve optare, invece, per l'accertamento di un concorso di colpa tra le parti quando si verifichi, da un lato, la presenza di indici di anomalia nell'operatività su home banking e, dall'altro lato, che il comportamento della parte ricorrente abbia colposamente collaborato con il truffatore, ad esempio cliccando su un link truffaldino (cfr. decisione Collegio di Torino n. 16061/2020 o n. 934/2021).
Si richiama seppure in modo sintetico lo "stato dell'arte" delle attuali strategie e tecniche con le quali soggetti malintenzionati possono tentare accessi fraudolenti a server esposti al Web, quali ad esempio account di home banking. Molteplici sono le tecniche fraudolente da parte di malintenzionati per indurre utenti privati a fornire, anche inconsapevolmente, informazioni utili per comprendere le credenziali di accesso a servizi informatici, compresi quelli di pagamento, come quello oggetto di ricorso. Le principali tecniche di frode possono essere racchiuse in alcune macrofamiglie: attacchi Phishing, attacchi Spoofing, e attacchi Man in the middle.
Per quanto concerne il phishing, con questo termine si indicano le frodi basate su una vera e propria "pesca digitale", nella quale si diffondono messaggi digitali (tipicamente email) con template e formattazioni tipiche dell'Istituto Bancario o Ente del quale si ambisce conoscere le credenziali di accesso. Alcuni utenti vengono convinti dalle email inviate, ove il destinatario della comunicazione pensando sia una comunicazione del proprio Istituto replica alla richiesta di informazioni. Tali azioni possono coinvolgere pochi utenti con invio di email ad-hoc sempre più di dettaglio o coinvolgere migliaia di contatti email in mailing list nelle disponibilità dell'attaccante. Non è infrequente che l'utente possa allentare la propria attenzione e cadere nella trappola di replicare alle medesime email con dati sensibili e che in seguito compongono per il criminale il puzzle delle credenziali di accesso necessario per l'azione fraudolenta atteso che tali messaggi digitali sono dotati il più possibile della veste grafica dell'Istituto bancario e con tono colloquiale aderente a quelli normalmente ricevuti. L'esperto della contraffazione sovente inserisce link (collegamenti digitali a server esterni) che apparentemente consentono di accedere al sito Web autentico dell'Istituto bancario, ma che di fatto conducono a siti web contraffatti (identici a quelli oggetto di mira fraudolenta) o persino a finestre a comparsa (pop-up) dall'aspetto identico alla rispettiva ufficiale: tali siti web e link web contraffatti sono definiti "spoofed" (falsificati), da cui il termine attacchi spoofing.
Al riguardo, sembra opportuno precisare che quando si parla di spoofing si intende fare riferimento a una forma di aggressione informatica che consiste nella manipolazione dei dati relativi al mittente di un sms per far sì che esso appaia provenire da un soggetto differente, mediante la sostituzione del numero originario con un testo alfanumerico

riconducibile a quello utilizzato dall'intermediario per i propri messaggi genuini. Dal canto suo invece, il caller-id spoofing ricorre allorquando la chiamata telefonica effettuata dal falso operatore appare riferibile a una utenza della banca. Scendendo più nel dettaglio, è da rilevare che, nella sua concreta concatenazione, la truffa suole svilupparsi nei seguenti termini: attraverso l'sms truffaldino (apparentemente proveniente dall'intermediario), il cliente viene anzitutto sollecitato a comunicare i propri dati e credenziali statiche (spesso cliccando sul link riportato nel messaggio); dopodiché, con la successiva chiamata (talvolta solo di vishing, ovvero di phishing telefonico), lo si induce a comunicare i codici otp trasmessi sul suo cellulare dalla banca in seguito alla inizializzazione della operazione compiuta dal malfattore (utilizzando i dati precedentemente acquisiti), per lo più facendogli credere che occorre sventare un pagamento fraudolento in corso oppure aggiornare i dispositivi di sicurezza.
Tra le tecniche fraudolente si annoverano anche gli attacchi MITM (Man in the middle), con cui i malintenzionati riescono ad intercettare ed entrare nella connessione tra l'utente e il server del servizio; pertanto ogni comunicazione che l'utente invia all'Istituto e viceversa viene prima acquisito dal servizio informatico che si è frapposto e poi per non destare sospetti rinviato al destinatario originale.
A fronte di tale quadro appena abbozzato ed in continua evoluzione ed affinazione, in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici è quindi del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo.
Il Collegio alla luce di quanto sopra esposto richiama il principio secondo cui le banche svolgono attività professionale e devono adempiere tutte le obbligazioni assunte nei confronti dei propri clienti con la diligenza particolarmente qualificata dell'"accorto banchiere", non solo con riguardo all'attività di esecuzione di contratti bancari in senso stretto, ma pure in relazione a ogni tipo di atto o di operazione oggettivamente esplicate. Perciò, la banca è responsabile fino a prova contraria dell'approntamento dei mezzi meccanici, dell'idoneità e funzionamento dei relativi servizi, in modo tale che la banca non può liberarsi dal dovere di tenere un comportamento che si attesti sul livello di professionalità dell'"accorto banchiere".
A tale ultimo proposito l'intermediario ha riferito che le operazioni contestate sono state autenticate tramite OTP dispositiva, a seguito di accesso all'area riservata e di *enrollment* di un nuovo *device*.
La resistente ha precisato che per accedere al Servizio di Internet Banking, occorre inserire i seguenti codici:

- Codice Identificativo Utente (c.d. "User ID") fornito dalla Banca e non modificabile dal cliente;
- Password di Accesso (c.d. "PIN"): codice alfanumerico che solo il cliente conosce e può modificare;
- OTP Login: password generata da dispositivo *** Pass Code o *** token per accedere all'Area Riservata;
- OTP Dispositivo: password generata da dispositivo *** Pass Code o *** token per confermare gli ordini di pagamento disposti dal cliente.

Ha poi riferito che la cliente, in fase di sottoscrizione del contratto, ha scelto, quale strumento di autenticazione, il dispositivo *** Pass Code, vale a dire un software capace di generare codici temporanei 'usa e getta' (OTP: One Time Password) che vengono richiesti sia per accedere all'Area riservata dell'Internet Banking sia per confermare le disposizioni di pagamento.
Il Collegio rileva che circa la prova della corretta autenticazione della operazione di *enrollment* - quale antecedente necessario delle operazioni contestate - l'intermediario ha riferito che alle ore 19.48 è avvenuta la disinstallazione della licenza del *token software* I** *Pass Code"* dal dispositivo X** R** Note 8 avente IP 2.32.*** e un *enrollment* del *token* su diverso *device* H. H.-L09 associato ad un altro indirizzo IP 5.171.***. Tale operazione è stata possibile grazie al codice di attivazione della licenza che è stato inviato all'indirizzo *email* della cliente odierna ricorrente.
Vi è quindi una esplicita confessione del fatto che l'associazione del nuovo *device* è stata portata a termine con un codice trasmesso via email.
Il Collegio, evidenzia, però con valore dirimente al fine del decidere che, sulla base dell'Opinion dell'EBA e delle tabelle ad essa allegata (specificatamente la table 3 rubricata Non-exhaustive list of possible knowledge elements) l'email non è considerato un elemento valido ai fini della SCA.
Come è noto il 21 giugno 2019 l'Autorità Bancaria Europea (EBA) ha emanato la Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, con cui ha precisato, ai fini dell'implementazione del Regolamento n. 2018/389, quali elementi costituiscano o meno, allo stato attuale della tecnologia, fattori di autenticazione forte all'interno delle categorie della conoscenza, del possesso e dell'inerenza.
Il quadro normativo relativo alla materia in argomento va, infatti, necessariamente integrato, ai fini di una compiuta valutazione della questione in esame, dai pertinenti interventi dell'Autorità Bancaria Europea, in termini di Opinion (in particolare la suddetta Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, nonché le tabelle allegate), di Linee guida (in particolare le Guidelines on outsourcing arrangements), di chiarimenti forniti in risposta a quesiti (Q&A).
Il Collegio ritiene, alla luce del corredo documentale in atti, non provato che il sistema adottato da parte resistente sia adeguato a SCA.
Come è noto, infatti, per innalzare i livelli di sicurezza e chiarire gli obblighi minimi a carico dei prestatori dei servizi la direttiva PSD2, n. 2015/2366/UE, recepita dall'Italia con d.lgs 218/2017 (entrato in vigore il 13.01.2018) ha introdotto la cd. autenticazione forte del cliente (Strong Customer Authentication - SCA).
Si tratta di una procedura per convalidare l'identificazione di un utente basata sull'uso di due o più elementi di autenticazione (cd. "autenticazione a due fattori"), appartenenti ad almeno due categorie tra le seguenti:
- conoscenza (qualcosa che solo l'utente conosce, come una password o un PIN);
- possesso (qualcosa che solo l'utente possiede, come un token/chiavetta, o uno smartphone);
- inerenza (qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale).
Questi elementi devono essere indipendenti tra loro, in modo che un'eventuale violazione di uno di essi non comprometta l'affidabilità degli altri.
Pertanto alla luce delle risultanze documentali sopra richiamate deve senz'altro affermarsi la responsabilità dell'intermediario resistente in ordine al danno lamentato dalla parte ricorrente, conformemente al prevalente orientamento ABF secondo il quale, in caso di operazioni bancarie effettuate a mezzo di strumenti elettronici, la non corretta operatività

del servizio bancario mediante collegamento telematico, ivi compresa la possibilità di una abusiva utilizzazione delle credenziali di accesso da parte di terzi, rientra nel rischio d'impresa della banca intermediaria. Su quest'ultima grava pertanto una responsabilità di tipo oggettivo, dalla quale la banca va esente solo provando che le operazioni contestate dal cliente sono attribuibili a dolo o colpa grave di quest'ultimo e comunque abbia provato quale intermediario di essersi comunque dotato di un procedimento pluri-fattoriale di autenticazione delle operazioni di pagamento secondo i parametri-base della c.d. PSD2 e dell'EBA, costituendo essa un *prius* logico rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.
La domanda della parte ricorrente merita pertanto accoglimento, atteso che la predisposizione da parte dell'intermediario di un sistema di autenticazione forte per l'operatività su conto on line di per sé rappresenta, come dedotto, il minimo della cautela pretesa dal legislatore per evitare che il prestatore di servizi di pagamento risponda in ogni caso (quindi anche nell'ipotesi di colpa grave del pagatore) di qualsiasi operazione non autorizzata, salva la frode ai sensi dell'art. 12.2-bis del d.lgs. 11/2010.
Era, al sommar di tutto, onere di parte resistente dover provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento sulla base di un principio di buona fede nell'esecuzione del contratto. In assenza di tale prova è corretta la decisione di imputare all'intermediario il rischio professionale della possibilità che terzi accedano ai profili dei clienti con condotte fraudolente.
Il Collegio riconosce, quindi, a parte ricorrente l'integrale rimborso della somma sottratta.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 12.000,00.
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
EMANUELE CESARE LUCCHINI GUASTALLA