Tribunale|Firenze|Sezione 3|Civile|Sentenza|23 novembre 2022| n. 3282

Data udienza 22 novembre 2022

Integrale

Contratti e servizi bancari - Servizi di pagamento - Operazioni digitali - Misure di sicurezza - Corretta autenticazione - Onere della prova

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

IL TRIBUNALE DI FIRENZE

TERZA SEZIONE CIVILE

nella persona del Giudice dott. …. ha pronunciato la seguente

SENTENZA

nella causa civile di I Grado iscritta al n. r.g. 591/2020 promossa da:

(...) (C.F. (...)), con il patrocinio dell'avv…...

ATTORE

contro

(...) SPA (C.F. (...)), con il patrocinio dell'avv. ….

CONVENUTO

RAGIONI DI FATTO E DI DIRITTO DELLA DECISIONE

(...) ha convenuto in giudizio (...) s.p.a. al fine di ottenere la restituzione della somma di Euro 83.700,00 oltre interessi, fuoriuscita dal conto a seguito dell'esecuzione di alcuni bonifici non autorizzati.

A fondamento della domanda ha allegato:

- che l'attrice, di 86 anni, confidando nel rapporto di fiducia instaurato con l'ex direttore di filiale della (...) di cui la (...) era cliente, (...), aveva deciso nel 2014 di trasferire i propri risparmi presso la (...) dove il (...) prestava la propria attività di consulente finanziario, lasciando invece il conto corrente presso (...) per l'accredito della pensione e le spese correnti;

- che il c/c n. (...) venne aperto presso la Filiale 1 di (...), Piazza….. n. …. con l'aiuto del predetto consulente e che lo stesso venne utilizzato quale conto corrente d'appoggio per effettuare un investimento della somma di Euro 100.000,00 (sottoscritto il 6.3.2014, che prevedeva una scadenza al 27.3.2017);

- che l'attrice, su sollecitazione del consulente finanziario (...), era stata convinta a richiedere alla banca una chiavetta o-key per compiere eventuali operazioni di home banking, nonostante non avesse le competenze tecniche necessarie per effettuare operazioni in autonomia;

- che l'attrice, smarrita la chiavetta, fu sollecitata dal (...) a chiederne un'altra, recapitata nel gennaio 2017 e consegnata direttamente dal consulente;

- che dopo la naturale scadenza degli investimenti (27.3.2017) l'attrice si recò personalmente presso la filiale della Banca per verificare l'effettivo accredito della somma investita e in tale occasione scoprì che sul conto corrente vi era solo la somma di Euro 936,00 e, a seguito degli accertamenti richiesti, apprese che vi era stato un disinvestimento anticipato non autorizzato e che erano stati eseguiti sei bonifici non autorizzati per un ammontare di Euro 83.700,00 in favore di tale (...) con causali prive di giustificazione;

- che le operazioni non autorizzate sono state le seguenti:

bonifico internet del 13/02/2017 di 24.800,00 Euro a favore di (...) con causale "rimborso spese immobile" - CRO: (...);

bonifico internet del 13/02/2017 di 24.900,00 Euro a favore di (...) con causale "rimborso spese immobile" - CRO. (...);

bonifico internet del 15/02/2017 di 7.500,00 Euro a favore di (...) con causale "consulenza progettazione" - CRO: (...);

bonifico internet del 15/02/2017 di 7.500,00 Euro a favore di (...) con causale "consulenza progettazione" - CRO: (...);

bonifico internet del 15/02/2017 di 9.500,00 Euro a favore di (...) con causale "spese forfettarie professionista" - CRO: (...);

bonifico internet del 15/02/2017 di 9.500,00 Euro a favore di (...) con causale "spese forfettarie professionista" - CRO: (...);

- che in data 21.4.2017 la (...) ha presentato denuncia-querela alla Procura della Repubblica di Firenze e all'esito delle indagini sono state rinviate a giudizio quattro persone tra cui il consulente finanziario (...) e la destinataria dei bonifici (...);

- che i tentativi di risoluzione bonaria della lite non sono andati a buon fine e la Banca non ha neppure partecipato al procedimento di mediazione tenendo pertanto una condotta contraria a buona fede;

- che sussiste la responsabilità della Banca ex art. 11 D.Lgs. n. 11 del 2010 non essendo i bonifici riconducibili all'attrice;

- che l'attrice non avrebbe potuto effettuare i bonifici perché sono state a sua insaputa cambiate le credenziali di accesso (PIN) e di sicurezza/controllo (numero di telefono presso cui ricevere l'sms di sicurezza per autorizzare le operazioni di disposizione);

- che la Banca non ha adottato adeguati presidi di sicurezza per scongiurare una fraudolenta sostituzione di persona ed ha consentito alla compagna convivente di (...), (...), rinviata a giudizio, qualificatasi per la signora (...), di ottenere per telefono il cambio delle credenziali di accesso al fine di effettuare poi la modifica del numero telefonico presso cui ricevere l'sms di sicurezza;

- che la Banca non ha avvertito l'attrice dell'esecuzione di operazioni sospette e che presentavano indici di anomalia tenuto conto dell'età e del comportamento pregresso dell'attrice;

- che la Banca ha acconsentito il disinvestimento anticipato dei titoli per un valore di 100.000,00 non autorizzato.

La Banca si è costituita in giudizio ed ha chiesto il rigetto della domanda in quanto infondata e non provata e, invia subordinata, ha chiesto l'accertamento della responsabilità "esclusiva, preponderante o concorrente" dei parte attrice ex art. 1227, comma 1 c.c..

L'istituto di credito non ha contestato in maniera specifica il fatto che le operazioni dispositive non siano state effettivamente eseguite dal correntista ma ha dedotto che il danno sarebbe riconducibile in via esclusiva, stante in decisivo apporto causale, o -in ipotesi- concorrente alla condotta gravemente colposa tenuta dal correntista.

In proposito, la Banca ha dedotto:

- che l'attrice ha sottoscritto un contratto di home-banking pur non avendo alcuna competenza informatica e capacità di operare in autonomia;

- che ha consegnato i dispositivi (chiavetta) ed i codici di accesso al consulente finanziario contravvenendo ai doveri di custodia e segretezza, rendendo così possibile il cambio dei precedenti codici, l'effettuazione dei disinvestimenti e dei bonifici; che il (...) aveva pieno accesso al sistema di home banking della correntista al quale avrebbe invece dovuto accedere solo la medesima;

- che la cliente non ha tempestivamente denunciato il furto/smarrimento della password, delle credenziali e dei codici in suo possesso;

- che non sussiste alcuna responsabilità della Banca il cui sistema informatico non presenta alcuna falla, né è stato penetrato da terzi in maniera fraudolenta;

- che i bonifici sono risultati tutti pienamente regolari e, più precisamente, sono stati effettuati con le credenziali, le password e i codici assegnati dalla Banca in maniera esclusiva e riservata, anche previo invio di SMS all'utenza cellulare comunicata alla stessa (one time password). L'intera procedura in base alla quale è stato impartito ed autorizzato ciascun bonifico è stata conforme alle misure di sicurezza previste dalla (...) a norma di legge;

- che la Banca non avrebbe potuto bloccare i bonifici in quanto non emergevano elementi di particolare anomalia;

All'udienza del 10.11.2020 le parti si sono riportate ai rispettivi atti e l'attore, in particolare, ha precisato la domanda evidenziando come la Banca debba rispondere anche ai sensi dell'art. 2049 c.c. essendo (...) un private banker e consulente finanziario di (...).

La causa è stata istruita con produzioni documentali e, rigettata la richiesta di CTU, all'udienza del 12.7.2022 è stata trattenuta in decisione, previa assegnazione dei termini di cui all'art. 190 c.p.c.

1. La domanda avanzata dall'attrice impone una preliminare disamina della responsabilità della banca per utilizzo abusivo degli strumenti di pagamento.

Le disposizioni normative in tema di gestione dei servizi bancari di pagamento si rinvengono nel D.Lgs. n. 11 del 2010 emanato in recepimento della direttiva europea 2007/64/CE, cd. PSD -

Payment Services Directivem, poi modificato dal D.Lgs. n. 218 del 2017 (entrato in vigore il 13.01.2018) in attuazione della cd. direttiva PSD2.

La normativa si pone l'obiettivo di favorire l'utilizzo e la diffusione degli strumenti di pagamento diversi dal contante tramite un sostanziale innalzamento dei livelli di sicurezza delle operazioni, delineando gli obblighi di comportamento a carico dell'intermedio e dell'utente, il regime di responsabilità e l'allocazione del rischio in caso di operazioni fraudolente.

Le disposizioni maggiormente rilevanti sono le seguenti:

L'art. 7 delinea quelli che sono gli obblighi a carico dell'utente ovvero l'utilizzo in conformità al contratto degli strumenti di pagamento, la tempestiva comunicazione alla banca in caso di smarrimento, furto, appropriazione indebita o uso non autorizzato dello strumento, l'adozione di misure idonee a garantire la sicurezza e l'adeguata custodia dei dispositivi in dotazione.

L'art. 8 descrive invece gli obblighi a carico del prestatore del servizio. In particolare, va sottolineata la necessità di assicurare che i dispositivi "non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento", fatti salvi i doveri di custodia previsti dall'art. 7 D.Lgs. n. 11 del 2010 cit..

La Banca è quindi tenuta ad adottare le misure più idonee, alla luce dello sviluppo tecnologico, necessarie per impedire l'utilizzo abusivo dello strumento di pagamento.

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. n. 218 del 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.

Ancorché tali elementi siano stati introdotti solo a partire dalla direttiva PSD2, non applicabile ratione temporis al caso che ci occupa, la giurisprudenza e anche l'Arbitro Bancario e Finanziario hanno comunque ritenuto l'adozione di tale standard esigibile, alla luce dell'evoluzione tecnologica, anche nel periodo immediatamente precedente.

Del resto, il fatto che la direttiva fosse già stata emanata all'epoca dei fatti di cui si discorre, ancorché non fosse ancora scaduto il termine per la trasposizione nell'ordinamento interno, dimostra comunque come il sistema di autenticazione forte fosse già diffuso e fosse un'esigenza di sicurezza sentita, anche alla luce delle forme sempre più sofisticate di truffa.

Chiariti gli obblighi in capo alle parti, l'art. 10 individua i criteri di ripartizione dell'onere probatorio e dei rischi.

A fronte dell'allegazione da parte dell'utilizzatore che una determinata operazione di pagamento sia stata eseguita, il prestatore del servizio è tenuto a fornire la prova "che l'operazione di pagamento e' 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".

Anche qualora il prestatore offra tale prova non va per sé solo esente da responsabilità. Infatti, il comma 2 prevede che "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sè necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, ne' 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".

In altri termini, ancorché il prestatore dimostri che l'operazione è stata autorizzata nel rispetto delle procedure di autenticazione previste dalla banca, e che quindi sia giuridicamente imputabile all'utente, da tale circostanza non si può direttamente inferire che sia quest'ultimo a versare in colpa grave in relazione agli obblighi posti dall'art. 7, ovvero che abbia, ad esempio, incautamente comunicato le credenziali a soggetti terzi. Non si può pertanto ritenere che la pressoché totale invulnerabilità del sistema di autenticazione forte a "due fattori" sia tale di per sé a fondare la presunzione di una colpa grave in capo al cliente, in assenza di altri elementi di prova.

Tenuto conto che la condotta tenuta dal cliente è una circostanza non agevolmente dimostrabile dalla Banca, perché ricade nella sola sfera di conoscenza dell'utente, si può tuttavia ritenere che, seppure l'adozione dell'intermediario di valide ed efficaci misure di sicurezza non costituisca di per sé una prova liberatoria, eleva tuttavia il livello delle allegazioni richieste al cliente, al fine di rendere adeguatamente verosimile il carattere fraudolento dell'operazione (in questo senso ex multis, ABF, Coll. Napoli, decisione 27 marzo 2013, n. 172).

Nell'ipotesi in cui all'esito del giudizio non emergano tuttavia in maniera chiara le modalità fraudolente (cd. rischio da ignoto tecnologico), sulla base della ripartizione dell'onere probatorio, la responsabilità ricadrà comunque sulla Banca.

Ciò è conforme alla regola di ripartizione di responsabilità posta dall'art. 10 e alla ratio legis risultando equo oltreché economicamente efficiente, anche al fine di promuovere negli utenti la fiducia nell'utilizzo degli strumenti di pagamento elettronici, ricondurre nell'area del rischio professionale del PSP i casi di utilizzo fraudolento degli strumenti di pagamento non riconducibili al dolo o alla colpa del titolare, né a un grave carenza dei presidi di sicurezza predisposti dall'intermediario. La Banca è infatti, è in grado, molto più che il singolo utente, di valutare la dimensione del rischio al fine non solo di adottare i presidi di sicurezza più evoluti ed efficaci per contenerlo, ma anche per tradurlo in un costo economicamente sostenibile (stipulando ad esempio contratti di assicurazione).

In questi termini si è espressa la giurisprudenza di legittimità che, dopo aver ricondotto la fattispecie nell'alveo della responsabilità contrattuale, ha affermato che: "in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è 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. Ne consegue che, anche prima dell'entrata in vigore del D.Lgs. n. 11 del 2010, attuativo

della direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, la banca, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente (Cass. 16417/2022; Cass. 9158/2018; Cass. 2959/2017).

2. Venendo al caso di specie, la Banca è quindi gravata da un duplice onere: in primo luogo deve provare "che l'operazione di pagamento e' 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";

ove tale prova sia raggiunta, per andare esente da responsabilità, deve provare il dolo o la colpa grave dell'utente (art. 10).

2.1. In ordine al primo profilo, non è oggetto di contestazione che i bonifici siano stati, formalmente, effettuati con le credenziali, le password e i codici assegnati dalla Banca in maniera esclusiva e riservata, anche previo invio di SMS all'utenza cellulare comunicata (v. pag. 12 comparsa).

Parte attrice contesta però l'operato della Banca con riferimento al cambio non autorizzato dell'utenza telefonica su cui ricevere l'OTP.

Dalla "Guida ai servizi F." prodotta dalla Banca (doc. 3) risulta che l'istituto di credito si era dotato di un sistema di autenticazione forte a due fattori, per le operazioni dispositive, basato sui seguenti codici di identificazione:

- codice titolare e codice pin (conosciuti solo dall'utente);

- codice o-key, generato dalla chiavetta (che solo l'utente possiede).

La Banca aveva però approntato un ulteriore presidio "per rafforzare il livello di sicurezza di alcune disposizioni di pagamento che la Banca considererà non abituali e quindi sospette" prevedendo, in tal caso, la necessità di inserire "oltre al codice o-key, anche un codice di sicurezza che verrà inviato gratuitamente via sms".

Per le operazioni, valutate automaticamente dal sistema come sospette, la Banca prevedeva quindi tre fattori di autenticazione (codice utente-pin, token-chiavetta e codice inviato via sms). La guida chiarisce altresì che "il numero di cellulare a cui sarà inviato il codice sms è quello memorizzato" e che "per maggiore sicurezza, anche la procedura di variazione di questo numero prevede l'inserimento di un codice sms che verrà inviato al numero che si desidera modificare. A variazione avvenuta, un sms confermerà l'avvenuta variazione".

Orbene, è pacifico che le operazioni effettuate sono state individuate dal sistema informatico della banca come non abituali e quindi sospette, motivo per cui è stato richiesto l'inserimento di un ulteriore codice inviato tramite sms.

Il presidio di sicurezza non ha però funzionato perché antecedentemente il truffatore era riuscito a modificare il numero di cellulare abbinato sfruttando una falla del sistema della banca.

Dall'indagine eseguita dalla Guardia di Finanza è emerso che il 13.2.2017 alle ore 11.22 G.D., compagna del (...), sostituendosi falsamente alla (...), aveva contattato il call center della banca al fine di ottenere il reset del PIN, certificando la propria identità (doc. 18 attrice)

Il reset del PIN comporta l'azzeramento di tutte le credenziali (ed anche del numero di cellulare precedentemente inserito) nonché la necessità di effettuare un nuovo accesso on-line (v. pag. 3 doc. 3 convenuta). L'espletamento di una nuova procedura di primo accesso comporta che il sistema richieda nuovamente la personalizzazione del codice PIN nonché la necessità di effettuare "nuovamente anche il primo accesso al servizio sms a richiesta, utilizzando i nuovi codici ricevuti".

Effettuato il reset del PIN, il truffatore ha quindi effettuato un nuovo accesso e "con procedura telematica che ha richiesto l'uso del dispositivo o-key è stato effettuato l'accesso per inserire l'utenza (...)" (relazione GdF del 9.12.2017 - doc. 18) il medesimo giorno e poi il successivo 15 febbraio 2017 ha effettuato i bonifici oggetto di contestazione.

In altri termini, tramite il possesso della chiavetta OTP -su cui si dirà meglio in appresso- e la conoscenza del PIN e del codice titolare è stato possibile per il truffatore, tramite una procedura di reset effettuabile telefonicamente, cambiare anche il numero di cellulare di riferimento.

Ora, se l'inserimento del codice OTP inviato all'utenza telefonica mobile personale del correntista via sms rappresenta il presidio di sicurezza previsto proprio per le operazioni che la Banca identifica come "non abituali e quindi sospette" la modifica del numero di telefono da utilizzarsi per tale autenticazione costituisce un'operazione che deve essere particolarmente protetta.

Dal momento in cui si consente invece la modifica del numero di cellulare tramite una semplice procedura di reset effettuabile telefonicamente (attraverso la mera comunicazione degli altri codici identificativi) di fatto si rende inefficace il presidio di sicurezza aggiuntivo approntato.

Si dirà che al momento del nuovo "primo accesso" l'utente deve comunque inserire il codice generato dalla chiavetta O-key e quindi è previsto un sistema di autenticazione forte a due fattori (codice titolare - token). Tuttavia, a tale obiezione si può replicare che è la stessa Banca che riconosce che tale sistema, nei casi maggiormente sospetti, può non risultare sufficiente, e risulta pertanto necessario richiedere un terzo presidio di sicurezza (codice inviato via sms).

In ogni caso, al di là degli obblighi nascenti dalla normativa speciale e codicistica (ex art. 1176, comma 2 c.p.c.), nel caso di specie l'obbligazione ha fonte contrattuale. Si legge nella guida ai servizi della banca, vigente all'epoca dei fatti (doc. 3 banca), che "per maggiore sicurezza, anche la procedura di variazione di questo numero prevede l'inserimento di un codice sms che verrà inviato al numero che si desidera modificare. A variazione avvenuta, un sms confermerà l'avvenuta variazione".

L'istituto di credito aveva pertanto già assunto l'obbligo contrattuale di adottare un ulteriore sistema antifrode relativamente alla modifica del numero di cellulare (necessario per autorizzare le operazioni sospette). Il reset del PIN (e delle credenziali) e il consequenziale inserimento di un nuovo numero di cellulare in sede di "nuovo" primo accesso, dal punto di vista sostanziale, è infatti perfettamente assimilabile ad una "variazione".

Il vulnus del sistema adottato dalla Banca sta quindi nel fatto che, sebbene per modificare il numero di telefono venga inviato un messaggio antecedentemente e successivamente all'operazione al numero inserito, tale sistema di sicurezza può essere aggirato facilmente attraverso il reset -per via telefonica- dei codici (pin e codice titolare) poiché in tal caso, al nuovo accesso, si potrà inserire un nuovo numero di cellulare senza che venga dalla banca inviato alcun sms al numero precedentemente inserito.

Provato l'inadempimento, "l'accertamento del nesso causale postula un giudizio controfattuale, fondato sul principio sancito dall'art. 40 c.p., comma 2, volto a stabilire se l'osservanza di determinate regole, imposte da disposizioni di legge o regolamentari o da specifiche clausole contrattuali o dai canoni di diligenza e correttezza cui deve uniformarsi il comportamento delle parti, sarebbe risultato, secondo criteri di certezza probabilistica, idoneo ad impedire l'evento (Cass. 23197/2018; Cass. 12401/2013; Cass. 9067/2018).

Nel caso di specie, come osservato dall'attrice, se al momento della richiesta telefonica di reset del pin, o al momento dell'inserimento del nuovo numero telefonico, fosse stato inviato un "codice SMS" per confermare l'operazione (così come previsto per il procedimento on line di modifica), lo stesso sarebbe giunto sul cellulare dell'attrice e quindi il truffatore non avrebbe potuto procedere oltre.

Infatti, se fosse stata richiesta la variazione del numero di telefono utilizzando le credenziali di accesso senza operare il reset del pin il cambio non sarebbe mai avvenuto perché l'(...), come previsto dal regolamento della Banca, avrebbe ricevuto sul proprio numero di cellulare l'sms con il codice per autorizzare l'operazione.

Tenuto conto che i bonifici del 13.2.2017 hanno richiesto l'inserimento del codice inviato via sms, essendo quindi stati identificati come "non abituali e sospetti" (v. pag. 7, doc. 10 banca) la violazione delle obbligazioni assunte in ordine alla procedura di variazione del numero di cellulare di riferimento o comunque la mancata adozione dei medesimi presidi di sicurezza in caso di reset effettuata tramite call center ha avuto una indubbia efficacia causale nella produzione del danno.

Va precisato che le disposizioni del 15/2 sono state valutate probabilmente come "non sospette" e quindi non è stato necessario l'inserimento dell'sms OTP (v. pag. 7, doc. 10 banca) poiché nei giorni precedenti erano stati autorizzati bonifici verso il medesimo beneficiario anche con sms, ragione per cui l'operazione non poteva più considerarsi anomala e non abituale rispetto all'operatività del conto corrente. Senza l'autorizzazione -per mezzo dell'sms- dei primi bonifici, anche i successivi del 15.02 sarebbero stati però ragionevolmente qualificati dal sistema come non abituali, o comunque, ricevendo l'sms, il cliente si sarebbe certamente allarmato per cui il truffatore non avrebbe potuto procedere oltre.

A ciò si aggiunge un ulteriore elemento evidenziato dall'attrice sin dall'atto introduttivo, ovvero la mancata autorizzazione di tutte le operazioni di disinvestimento anticipato dei titoli.

Ebbene, parte convenuta non ha documentato se e come tali operazioni siano state autorizzata: se effettuate mediante home banking (come parrebbe dalle deduzioni in comparsa di costituzione) occorre rilevare che non risultano prodotti, perlomeno per i disinvestimenti antecedenti al 13.2.2017, le registrazioni nel sistema della Banca (doc. 10) da cui poter desumere l'effettiva autenticazione dell'utente; se, invece, come prospettato dalla Banca nella replica conclusionale (pag. 10), si è trattato di moduli cartacei sottoscritti dal cliente, l'istituto di credito avrebbe dovuto produrne copia in giudizio al fine di legittimare il proprio operato e assolvere al proprio onere probatorio, a fronte delle puntuali allegazioni dell'attrice (v. pag. 3 atto di citazione).

Né è condivisibile la tesi secondo cui i disinvestimenti in questione non avrebbero cagionato alcun danno, visto che le somme sono rimaste sul conto della cliente, rappresentando invero l'antecedente causale della sottrazione. Infatti, qualora le somme fossero rimaste vincolate, circostanza su cui

faceva affidamento l'attrice, i bonifici non si sarebbero potuti eseguire o perlomeno avrebbero potuto avere ad oggetto un importo inferiore.

2.2. Passando ad esaminare la condotta tenuta dal cliente, occorre valutare se le eccezioni formulate dall'istituto di credito consentano di ravvisare una colpa grave dell'attrice idonea ad interrompere il nesso causale o comunque a determinare un corso di colpa ex art. 1227 c.c.

2.2.1. La prima contestazione mossa dall'istituto di credito ha ad oggetto la comunicazione delle credenziali e la violazione dei doveri di custodia.

E' infatti pacifico che il truffatore fosse a conoscenza perlomeno del codice titolare e PIN della ricorrente poiché diversamente non sarebbe stato possibile procedere al reset, che ha poi consentito la variazione del numero telefonico per la ricezione degli sms.

Nel caso di specie, tuttavia, occorre considerare che non siamo di fronte a pagamenti fraudolenti effettuati da un truffatore ignoto o comunque estraneo, essendo pacifico che l'autore della sottrazione sia stato proprio il consulente (...), (...), in concorso con altri correi.

La circostanza emerge dagli atti del procedimento penale prodotti e non è contestata.

Il regime di responsabilità di cui al D.Lgs. n. 11 del 2010 si intreccia quindi con la disciplina prevista dall'art. 31 D.Lgs. n. 58 del 1998 e dall'art. 1228 c.c. (art. 2049 c.c.).

La giurisprudenza ha affermato che gli istituti di credito rispondono dei danni arrecati a terzi dai propri incaricati nello svolgimento delle incombenze loro affidate, quando il fatto illecito commesso sia connesso per occasionalità necessaria all'esercizio delle mansioni (Cass. 28634/2020).

Ciò non significa che nell'ipotesi in cui la truffa sia posta in essere dal consulente finanziario non possa mai assumere rilievo la colpa grave del cliente in relazione agli obblighi di cui all'art. 7 D.Lgs. n. 11 del 2010. Tuttavia, la qualifica rivestita dall'autore della sottrazione assume rilievo al fine di valutare l'intensità della colpa ovvero l'inescusabilità del comportamento del cliente.

E' stato infatti precisato che "la responsabilità dell'intermediario ai sensi del D.Lgs. n. 58 del 1998, art. 31, comma 3, per i danni arrecati ai terzi dai propri promotori finanziari deve essere esclusa ove il danneggiato ponga in essere una condotta agevolatrice che presenti connotati di anomalia, vale a dire, se non di collusione, quanto meno di consapevole acquiescenza alla violazione delle regole gravanti sul promotore (cfr. Cass., 28/7/2021, n. 21643; Cass., 15/12/2020, n. 28634; Cass., 12/10/2018, n. 25374; Cass., 10/11/2015, n. 22956; Cass., 13/12/2013, n. 27925; Cass., 24/3/2011, n. 6829; Cass., 24/7/2009, n. 17393; Cass., 7/4/2006, n. 8229), verificandosi in tal caso l'interruzione del nesso di occasionalità necessaria tra il fatto produttivo di danno e l'esercizio delle mansioni cui il promotore finanziario sia adibito (cfr. Cass., 28/7/2021, n. 21643; Cass., 12/10/2018, n. 25374), costituente condizione necessaria dell'intermediario" (Cass. 34789/2021).

Ebbene, dalla disamina della stessa giurisprudenza richiamata dall'istituto di credito (v. pag. 9 comparsa conclusionale) ritiene il Tribunale che, nel caso di specie, il comportamento tenuto dalla (...) non possa ritenersi talmente anomalo da dimostrare una "consapevole acquiescenza alla violazione delle regole gravanti sul promotore".

L'attrice non ha infatti mai dichiarato di aver consegnato spontaneamente le credenziali di accesso al consulente così come la chiavetta token consentendo al consulente di operare in totale autonomia, né di aver instaurato un rapporto parallelo con il private banker rispetto a quello intercorso con la Banca. Ciò che invece è ammesso dall'attrice è che la stessa, non avendo conoscenze informatiche,

avrebbe operato sul conto on-line sempre con l'assistenza prestata dal (...) che si recava presso la sua abitazione per aiutarla. Pertanto, è ragionevole ritenere che proprio in tali occasioni il consulente abbia carpito le credenziali.

L'attrice ha documentato che sul sito internet (...) nella pagina "la relazione con il tuo private banker" era indicato testualmente: "È sempre a tua disposizione negli ambienti accoglienti e confortevoli dei suoi uffici oppure, se lo preferisci, comodamente a casa tua o nel tuo ufficio. Quale che sia il luogo, ti assiste nella gestione completa del patrimonio individuando soluzioni personalizzate e aiutandoti a utilizzare al meglio i servizi e la tecnologia della banca. Con la semplicità e la professionalità di cui hai bisogno".

Dal momento che la Banca consentiva ai consulenti di operare anche al di fuori della sede dell'istituto offrendo non solo un servizio di consulenza finanziaria ma anche un non precisato ausilio a "utilizzare al meglio i servizi e la tecnologia della banca" era evidente che si potessero creare situazioni di potenziale ingerenza nella sfera dell'utente.

Né si può ritenere, a fronte di tale offerta pubblicizzata dallo stesso istituto bancario, gravemente colpevole l'affidamento serbato dall'attrice nel rapporto professionale e fiduciario consolidato con il (...).

Del resto, l'istituto di credito, dal cui status professionale discendono obblighi di protezione per il cliente, non ha neppure provato quali fossero le modalità attraverso le quali i consulenti potevano fornire alle parti assistenza nell'utilizzo della tecnologia necessaria per avvalersi dei servizi della banca, anche a domicilio, scongiurando tuttavia il rischio che gli stessi, anche incidentalmente, potessero venire a conoscenza delle credenziali necessarie per l'accesso allo strumento di pagamento.

La lamentata violazione del dovere di custodia dei codici incombente sul cliente (art. 7 D.Lgs. n. 11 del 2010) va quindi valutata tenendo conto delle specifiche circostanze del caso di specie, ovvero:

- la posizione rivestita dal truffatore e le mansioni espletate anche in relazione all'assistenza nell'utilizzo dei servizi e della tecnologia della banca;

- il consolidato rapporto di fiducia con la cliente;

- il fatto che il consulente abbia operato fuori dai locali commerciali, presso l'abitazione della parte, dove si abbassa la soglia di attenzione e la buona fede del cliente può essere più facilmente aggirata;

- l'età e le scarse conoscenze informatiche.

E' irrilevante il questionario di profilatura prodotto dalla banca (doc. 9) atteso che, in disparte il fatto che i dati sono stati inseriti dal (...), nella presente controversia non si discute dell'adeguatezza dell'investimento e del profilo finanziario ma delle conoscenze relative all'utilizzo dei sistemi informatici di home banking.

Tali elementi non consentono di valutare la condotta della parte in termini di colpa grave, definita dalla giurisprudenza di legittimità come quella "straordinaria e inescusabile imprudenza, negligenza o imperizia, che si verifica in conseguenza della violazione non solo della diligenza ordinaria del buon padre di famiglia di cui all'art. 1176, 1 comma, c.c." - vale a dire di una persona di media avvedutezza e accortezza, consapevole dei propri impegni e delle relative responsabilità - ma anche di "quel grado minimo ed elementare di diligenza generalmente osservato da tutti": non dunque ogni contegno imprudente può far ritenere integrato questo grado di colpa, ma solo quello che

appaia inescusabile e che non trovi neppure spiegazione nella particolarità della vicenda (Cass., 19 novembre 2001, n. 14456; Cass., 13 ottobre 2009, n. 21679 - ABF, Coll. Coord., n. 5304/2013).

Nel caso di specie siamo, del resto, di fronte ad una parte che è stata riconosciuta vittima di truffa con sentenza, non passata in giudicato, dal Tribunale di Firenze n. 5181/2021 (produzione attrice del 15.7.22); pronuncia che è liberamente valutabile dal giudice nel presente procedimento unitamente a tutte le altre prove assunte, essendo stati altresì prodotti gli atti di indagine che hanno dato origine al procedimento.

2.2.2. Quanto all'utilizzo della chiavetta-token, secondo presidio di sicurezza individuato dalla Banca, il quadro fattuale è più complesso.

L'attrice, infatti, non ha mai dichiarato -e la banca non ha provato il contrario-di aver consegnato il token al consulente finanziario ed invero ha prodotto in giudizio una fotografia del medesimo (doc. 23) dichiarando di esserne ancora in possesso. Ha poi precisato di aver utilizzato il token sempre alla presenza del consulente finanziario ma presso la propria abitazione.

La Banca non ha fornito la prova di quale sia stato il token utilizzato ovvero se la chiavetta attualmente in possesso della (...) (doc. 23) o quella smarrita e in tal caso non ha chiarito perché non sia stata disattivata a fronte della nuova richiesta.

L'assenza di elementi probatori forniti dall'istituto di credito è significativa nel contesto fattuale rappresentato dall'attrice.

La (...) ha infatti esposto di non aver rinvenuto la chiavetta presso la propria abitazione e, sul presupposto di averla smarrita, di essere stata sollecitata dal (...) a chiederne un'altra, recapitata personalmente dal consulente finanziario, come emerge altresì dall'estratto conto nel quale è registrato un addebito per la nuova chiavetta il 4.1.2017, poco prima dei bonifici sospetti.

Tenuto conto che nel corso della perquisizione domiciliare del (...) sono state rinvenuti tre token per l'accesso online a rapporti bancari (...) diverse sono le ipotesi alternative prospettabili. Non si può escludere che la chiavetta "smarrita" sia stata sottratta dal (...) che, impossessatosi del nuovo token, avrebbe poi riconsegnato alla cliente quella originaria, non più attiva, o che comunque il medesimo sia riuscito, in virtù del ruolo ricoperto, ad evitare la disattivazione della prima chiavetta.

Del resto, seppure dalla sentenza penale (pag. 5) risulta che il (...) aveva in passato utilizzato la chiavetta per accedere al servizio home banking a casa della (...) (v. anche pag. 4 memoria ex art. 183, VI comma n. 1 attrice), tuttavia, le operazioni oggetto di contestazione, sono avvenute presso un internet point e quindi al di fuori della sfera di controllo dell'utente (doc. 18, punto 6, attrice).

Sta di fatto che sarebbe stato onere della banca dimostrare quale sia stata la effettiva chiavetta utilizzata. Essendo rimasti incerti i profili sopra delineati, anche sotto tale profilo, l'eccezione sollevata da (...) va disattesa in quanto non idonea a dimostrare, neppure in via presuntiva, la colpa grave del cliente in relazione alla consegna del token al consulente.

2.2.3. Neppure si può ritenere che la cliente abbia violato l'obbligo di tempestiva comunicazione alla banca dell'appropriazione dei codici e del dispositivo da parte di soggetti terzi e comunque dell'utilizzo non autorizzato.

Infatti, si è detto, che una volta smarrita la chiavetta del proprio conto la (...) aveva provveduto a richiederne una nuova (doc. 8 attore), con ciò consentendo alla banca di disattivare il precedente dispositivo (se poi ciò sia avvenuto non è noto). Quanto alle ulteriori credenziali (PIN e codice

titolare) l'esclusione della colpa grave in ordine alla condivisione delle stesse con il consulente ai fini dell'assistenza nell'utilizzo della tecnologia e dei servizi della banca assume carattere assorbente.

2.2.4 Quanto al mancato controllo del conto corrente e alla mancata tempestiva comunicazione dei bonifici effettuati illegittimamente va rilevato che è circostanza non contestata che il conto fosse utilizzato solo come appoggio senza dunque una regolare operatività. L'attrice non aveva pertanto motivo per recarsi in banca al fine di controllare il saldo del conto corrente prima della naturale scadenza dell'investimento. Né la Banca ha dimostrato l'invio di estratti conto o comunicazioni (anche in ordine ai disinvestimenti precedentemente effettuati) dai quali la parte potesse immediatamente rendersi conto di un andamento anomalo del rapporto.

2.2.5. Infine, in ordine alla dedotta negligenza e imprudenza della parte che avrebbe attivato un servizio home banking in assenza di conoscenze informatiche e quindi nell'impossibilità di operare secondo il livello di diligenza richiesto all'agente modello di riferimento, ritiene il Tribunale che l'imprudenza dell'attrice non assurga al livello di colpa grave.

Non è infatti contestata la circostanza che sia stato proprio il consulente finanziario dell'attrice, della cui condotta la Banca risponde ex art. 1228 c.c., a convincere la cliente ad attivare tale modalità di gestione del conto corrente, rappresentando il proprio ruolo anche di assistenza tecnica.

Sarebbe stato invero il consulente, a fronte della scarsa dimestichezza degli strumenti informatici, anche in ragione dell'età della cliente, a dover eventualmente suggerire altre modalità di gestione, più consone al profilo dell'utente. Sotto tale profilo è pertanto semmai la Banca ad aver violato gli obblighi di protezione nascenti dal proprio status professionale e dal principio di buona fede contrattuale (art. 1375 c.c.).

Né si può censurare il comportamento del cliente per non aver dichiarato alla Banca, in sede di sottoscrizione dei contratti e al momento del cambio della chiavetta assegnata (doc. 8 . modulo richiesta 29.12.2016), la mancanza di conoscenze informatiche.

Negli scritti finali afferma la difesa di parte convenuta che "F., ove messa a conoscenza dell'incapacità di controparte di approcciare un mezzo informatico, mai e poi mai avrebbe consentito l'accesso della (...) ai predetti servizi".

La Banca omette però di considerare che l'interlocutore diretto della (...) era proprio il (...) (che ha sottoscritto i contratti di apertura di c/c e di adesione ai servizi online, doc.ti 6 e 7 convenuta) e pertanto la stessa non aveva motivo di rappresentare tali circostanze a ulteriori soggetti non potendo certo prevedere la successiva condotta fraudolenta tenuta dal consulente.

3. Alla stregua delle considerazioni che precedono va affermata la responsabilità esclusiva della Banca non essendo provata la colpa grave del cliente.

.... va condannata a restituire la somma di Euro 83.700,00 oltre interessi legali dalla messa in mora (diffida del 8.2.2018) all'effettivo soddisfo.

4. Le spese di lite seguono la soccombenza.

I compensi vanno liquidati con applicazione dei valori prossimi ai medi di cui al D.M. n. 147 del 2022.

5. La Banca va altresì condannata alla sanzione ex art. 8, comma 4-bis D.Lgs. n. 28 del 2010, nella formulazione ratione temporis applicabile, per la mancata partecipazione alla mediazione senza giustificato motivo, non ritenendo sufficiente la comunicazione inviata, che dimostra invero una aprioristica chiusura non giustificata, considerato quanto poi emerso in giudizio ed il fatto che lo stesso istituto di credito, nella corrispondenza intercorsa aveva evidenziato che la posizione presentava "carattere di assoluta delicatezza e peculiarità" (doc.15 attore).

P.Q.M.

Il Tribunale di Firenze, definitivamente decidendo, ogni diversa domanda disattesa o assorbita così provvede:

1) condanna (...) s.p.a. al pagamento in favore di (...) della somma di Euro 83.700,00 oltre interessi legali dalla messa in mora (8.2.2018) al saldo;

2) condanna (...) s.p.a. all'integrale rifusione delle spese legali in favore di (...) che liquida in Euro 14.000,00 per compensi, Euro 786,00 per esborsi, oltre spese generali nella misura del 15%, IVA e CPA come per legge;

3) condanna (...) s.p.a. al versamento in favore dell'Erario della somma di Euro 759,00, importo corrispondente al contributo unificato dovuto per il giudizio, come prescritto dall'art. 8, comma 4-bis D.Lgs. n. 28 del 2010 per la mancata partecipazione al procedimento di mediazione senza giustificato motivo.

Così deciso in Firenze il 22 novembre 2022.

Depositata in Cancelleria il 23 novembre 2022.