REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

Il Tribunale di Torre Annunziata, Terza Sezione Civile, in persona del giudice dott. Salvatore Nasti, ha pronunciato la seguente

SENTENZA

nella causa civile scritta al numero di ruolo generale /**2021** avente ad oggetto*: responsabilità da inadempimento contrattuale per violazione della diligenza professionale della banca*;

tra

o il a Sorrento (NA) ed ivi residente al), rappresentato e difeso dagli Avv.ti (C.F.), e ( ) presso il loro studio in alla Via , ivi elettivamente domiciliato in virtù di procura in atti;

parte attrice

contro

a., con sede in °4, iscritto al Registro delle Imprese di al n.° capitale versato pari ad €. , in persona del suo quadro direttivo dott. autorizzato a rappresentare la Banca giusta delibera n. del 21.10.2021 del CdA di rappresentato e difeso, in virtù di mandato in atti, dagli avv.ti C.F. ed (, e con loro elett.te dom.to presso il loro studio in alla via n. ;

parte convenuta

CONCLUSIONI

Le parti concludono come da note in atti, cui per brevità si rinvia.

SVOLGIMENTO DEL PROCESSO E RAGIONI DELLA DECISIONE

Si da atto che la presente sentenza viene estesa senza la concisa esposizione dello "svolgimento del processo" e dunque ai sensi delle indicazioni del secondo comma dell'art.132 c.p.c. come modificato per effetto delll'entrata in vigore dell'art. 45 comma 17 della legge 18 giugno 2009 n. 69,

Pertanto, devono all'uopo considerarsi integralmente richiamati dalla presente pronuncia sia l'atto introduttivo che la comparsa che ogni altro atto del giudizio nonché le istanze di cui ai verbali di causa ed ogni altra attività ivi verbalizzata.

Il Sig. [redacted] che intrattiene con il [redacted] S.p.a. rapporto di conto corrente n.° [redacted] dal febbraio 2020 ha convenuto in giudizio, con atto di citazione notificato il 12/03/2021, l'istituto di credito per sentir accertare e dichiarare l'esclusiva responsabilità da inadempimento contrattuale per violazione della diligenza professionale della banca per non aver predisposto un adeguato sistema di protezione, a tutela dei correntisti che utilizzano l'internet banking, dalle frodi informatiche, per non aver annullato i bonifici fraudolenti e condannare così l'istituto di credito al pagamento di tutti i danni patrimoniali subiti dall'istante, che quantifica in € 24.800,00 o nella diversa misura determinanda dal Tribunale anche, se del caso, a mezzo CTU. Narra l'attore che il 03 agosto 2020 alle 16:48, riceveva tramite sms inviato apparentemente dal numero verde del [redacted] una comunicazione che lo invitava al cliccare su di un link per non meglio specificati motivi di sicurezza.

Il sig. [redacted] apriva il link accedendo attraverso l'inserimento di nome utente e password ad una pagina web che richiedeva l'inserimento dei suoi dati di carte di credito. Senza aver inserito alcun tipo di informazione, poiché sprovvisto di carta di credito, ne usciva. Nella stessa giornata veniva contattato da un sedicente operatore di [redacted] del Servizio Antifrode, il quale lo allertava di un presunto attacco hacker sul suo internet banking. Il giorno dopo l'istante veniva nuovamente contattato dal finto operatore che confermava come il c/c fosse sotto attacco e fossero stati disposti numerosi bonifici verso l'estero, invitandolo, perché venissero bloccati ed annullati, a comunicare i codici OTP che di volta in volta gli sarebbero stati inviati dalla banca tramite sms. L'istante provvedeva a comunicare i codici OTP al finto operatore, il quale attraverso ulteriori sms, gli confermava l'avvenuto blocco dei bonifici e lo sventato pericolo. Al termine di tale operazione il [redacted] contattava telefonicamente il [redacted] per avere ulteriore conferma dello sventato pericolo, ma l'istituto di credito gli comunicava che purtroppo era stato vittima di una truffa telematica e disponeva il blocco del conto corrente. L'istante chiedeva al [redacted] p.a. la restituzione dell'importo sottratto (pari ad €. 24.800,00), che la banca gli negava per la violazione da parte del [redacted] degli obblighi relativi all'utilizzo degli strumenti di pagamento ed alla conservazione delle credenziali di sicurezza personalizzate necessarie per le operazioni di pagamento. Il Sig. [redacted] si rivolgeva all'Arbitro Bancario Finanziario di Napoli al fine di ottenere stra-giudizialmente il ristoro dell'importo sottratto dai truffatori da parte del [redacted] Il collegio arbitrale partenopeo con decisione del 02.02.2021 accoglieva parzialmente il

ricorso dell'istante, accertando il diritto di risarcimento limitatamente ad €. 900,00 pari alla metà dell'importo di €. 1.800,00 per il quale non è riscontrabile l'uso dell'OTP, oltre interessi legali dalla data del reclamo, ritenendo sussistente la colpa grave del [redacted], il quale aveva provveduto a fornire personalmente ai truffatori telematici i codici OTP per autorizzare le operazioni.

Negli anni la giurisprudenza ha sempre riconosciuto, in caso di truffa telematica ai danni del correntista, una responsabilità dell'istituto di credito, in quanto quest'ultimo è obbligato ad apprestare una serie di misure di sicurezza tali da garantire un sistema di autenticazione forte a tutela della sicurezza dei sistemi di pagamento ed in particolare una responsabilità per l'esercizio di un'attività pericolosa ex art. 2050 c.c. Secondo la normativa in materia di pagamento degli strumenti informatici, D. Lgs n.° 11/2010, c.d. P.S.D. *Payment Services Directive* la banca è tenuta a rimborsare al cliente l'importo dell'operazione eseguita senza autorizzazione, salvo l'ipotesi in cui la banca riesca a dimostrare che l'utente abbia agito con dolo e colpa grave. Proprio sulla base di tale principio il collegio arbitrale partenopeo con decisione del 02.02.2021 ha ritenuto di accogliere solo parzialmente la domanda dell'odierno attore, richiamando proprio quanto previsto all'art 10 comma I del D. Lgs 11/2010".

Il collegio partenopeo, in base alla documentazione prodotta da ambedue le parti, ha osservato come "*...per quanto riguarda le operazioni dispositive, la procedura applicata dall'intermediario per autorizzare le stesse sembrerebbe prevedere, come elemento di "possesso", l'OTP e sms inviato all'utenza cellulare dell'utilizzatore. Tale procedura integra il cd. Fattore di Possesso. L'opinion inoltre richiede che: i due elementi su cui si fonda l'autenticazione siano indipendenti, nel senso che la compromissione di uno di essi non pregiudichi l'affidabilità dell'altro elemento; per le operazioni online, almeno uno degli elementi sia collegato dinamicamente con l'importo ed il beneficiario del pagamento (dynamic linking). In particolare, gli standard tecnici dettati dall'EBA con provvedimento del 23 febbraio 2017 specificano che il pagatore deve essere informato dell'importo e del beneficiario per il quale è stato generato il codice di autenticazione; quest'ultimo codice deve essere rigenerato ogni volta che uno dei due parametri sia modificato. I due requisiti paiono rispettati nel caso di specie, in particolare gli sms mediante i quali sono stati trasmessi gli OTP, quelli per i quali l'intermediario ha qui prodotto evidenza, specificano sia l'importo del bonifico sia il beneficiario. In tal modo, il ricorrente, che secondo quanto riferisce avrebbe creduto di interloquire con un operatore della banca, avrebbe potuto almeno avvedersi che gli OTP erano stati generati per la conclusione di operazioni a lui estranee, verso beneficiari sconosciuti...*". Dall'analisi eseguita dall' A.B.F partenopeo, emerge la colpa grave dell'odierno attore, il quale in spregio alle norme contrattuali e quelle del buon senso, aveva provveduto a fornire i codici OTP al cyber-truffatore nove volte, nonostante nelle condizioni generali del contratto di c/c

ed internet banking sia espressamente indicato come l'utente / correntista non debba mai fornire a nessuno i propri codici e password. La colpa grave del [redacted] è quanto mai evidente poiché non è dovuta solo dalla comunicazione dei codici OTP, ma anche dalla comunicazione del nome utente e password.

Allorquando il [redacted] ha cliccato sul link, indicato nel falso messaggio sms inviatogli, si sarà trovato in una schermata che riproduceva l'accesso alla piattaforma [redacted] it e che richiedeva la computazione del nome utente e password per accedere. In tal modo il truffatore otteneva le credenziali necessarie per superare i primi due blocchi ed accedere alla pagina personale dell'utente. Grazie a questa prima ingenuità, il truffatore ha potuto visionare i movimenti di conto dell'utente e quando il Sig. [redacted] lo richiedeva una dimostrazione di star interloquendo effettivamente con un operatore [redacted], il sedicente operatore [redacted] elencava tutti i movimenti di conto rassicurando il malcapitato. Con la piena libertà di operare sulla pagina dell'Internet Banking, il malintenzionato predisponeva una ventina di operazioni di bonifico chiedendo l'emissione dei codici OTP alla banca che attraverso sms li comunicava sul cellulare del [redacted]. I messaggi oltre alle "*one time password*" riportavano anche le indicazioni delle operazioni predisposte ed i beneficiari. Comunicazioni queste ultime che non lasciavano spazio ad interpretazioni diverse rispetto a quello che stava accadendo nella realtà poiché il testo di tutti i messaggi riportava la seguente dicitura "*...xxxxx è il codice per autorizzare il tuo bonifico di xxxx € a favore di xxxxxx...*", il testo in questione è quanto mai chiaro ed esaustivo e le informazioni contenute al suo interno potevano e dovevano instillare il dubbio nel cliente. Vi è almeno la colpa del [redacted] che non ha prestato attenzione al tenore dei messaggi ricevuti

Ll'art 6 delle condizioni generali di contratto, sottosezione II° lettera b numero 8 (depositate in atti), che il correntista ha sottoscritto ed accettato, ottenendo copia cartacea dell'edizione di settembre 2019 al momento della stipula del contratto di conto corrente (come da prove in atti). Nel citato art. si legge: "*...il Cliente è tenuto a custodire diligentemente e a mantenere segrete le chiavi di autenticazione nonché a custodire il Generatore OTP assegnato dalla Banca e/o ogni altro dispositivo o strumento ammesso dalla Banca che consenta la generazione degli OTP e/o del Codice Dinamico, nonché a non consentire ad alcuno di fare uso della OTP e/o del Codice Dinamico, in qualsiasi modo generato. Il Cliente è responsabile del corretto utilizzo delle chiavi di autenticazione, del Generatore di OTP e/o di ogni altro dispositivo o strumento ammesso dalla banca che consenta la generazione della OTP e/o del Codice Dinamico, e della OTP e/o Codice dinamico in qualsiasi modo generato*". Il succitato art. 6 è altresì da leggersi in combinato disposto con l'art 7 del D. lgs 11/2010 che sancisce come l'utilizzazione dello strumento di pagamento debba essere eseguita in conformità ai patti contenuti nell'accordo quadro che regola il servizio, nella

tempestiva denuncia di furto o smarrimento e nella custodia attenta dei dati d'accesso. Il Sig. r[illegible] fornendo le OTP al truffatore, (ignorando il tenore dei messaggi che [illegible] inviava), ha apertamente violato la clausola contrattuale. La Suprema Corte di Cassazione Civile, sez. III con ordinanza del 05.07.2019, n.° 18045, ha statuito che: "la *responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi ha natura contrattuale e, quindi, va esclusa se ricorre una situazione di colpa grave dell'utente*".

Con una recente sentenza del 17.05.2021, per una analoga controversia, il Tribunale di Gela II° sez. civile, ha statuito che se anche il D. lgs 11/2010 riconosce obblighi in capo all'istituto di credito per la responsabilità di operazioni non autorizzate e/o l'utilizzo non autorizzato di strumenti e servizi di pagamento, qualora la banca riesca a dimostrare il dolo o la negligenza dell'utente nella conservazione di password, nome utente ed OTP, non gli potrà essere riconosciuta alcuna responsabilità. Il caso sottoposto all'attenzione del giudice gelese è analogo all'odierna controversia in quanto l'utente del servizio lamentava la sottrazione di somme di denaro dal proprio conto corrente, a fronte di una truffa di *phishing*, chiedendo il rimborso alla banca convenuta. Orbene il Tribunale di Gela ha rilevato come, nella specie, i sistemi di sicurezza utilizzati dalla banca resistente fossero pienamente efficaci e che soltanto la cooperazione del ricorrente, benché posta in essere non scientemente con gli autori dell'illecito, avesse reso possibile l'autorizzazione non voluta delle disposizioni di pagamento. Invero, una volta che l'istituto di credito avvisa l'utente, per il tramite del sistema di sicurezza, dello svolgimento di una specifica operazione e gli trasmette il codice di autorizzazione, è rimessa all'utente la scelta di utilizzare i codici, così dando corso all'operazioni o arrestarsi revocandole. In definitiva, l'autorizzazione della disposizione di pagamento dipende unicamente dall'inserimento dei codici da parte dell'utente, senza i quali le operazioni non potrebbero essere portate a compimento. Nel caso di specie la colpa risulta addirittura aggravata dalla reiterazione del contegno del [illegible], che ha ripetutamente rivelato i codici di accesso di ciascuna operazione, di volta in volta comunicati tramite il sistema di sicurezza della banca resistente, senza avvedersi della disposizione di pagamento che tramite l'inserimento di essi andava ad autorizzare e delle quali nei messaggi erano contenuti la tipologia, l'importo ed il beneficiario. Il sistema di sicurezza del [illegible] S.p.a. risulta efficace ed in linea con il sistema bancario nazionale ed europeo, soprattutto alla luce della normativa europea PSD2 che ha introdotto, per far fronte al crescente utilizzo di internet banking ed e-commerce, il sistema della Strong Customer Authentication (SCA) o Autenticazione Forte1 richiamata anche dalla Circolare n. 285 del 17 dicembre 2013 della Banca d'Italia. Proprio in virtù di tale normativa il sistema di

sicurezza predisposto dal [redacted] S.p.a. non si presta ad alcuna censura in quanto strutturato su di un sistema cosiddetto a tre livelli (nome utente, password ed OTP) come previsto dalla normativa e circolare succitate.

Essendo la diffusione del fenomeno di portata tale, è ormai orientamento consolidato in giurisprudenza quello di ritenere l'impiego di una media diligenza da parte della clientela sufficiente a scongiurare il pericolo ed impedire la truffa con la conseguenza che la mancanza della stessa (come nel caso che ci occupa) rende immeritevole di accoglimento la domanda di risarcimento.

Ritiene lo scrivente magistrato che la questioone trattatta e l'avanzare della tecnologia e delle truffe informatiche più frequenti nel periodo moderno giustificano la compensazione delle spese

PQM

Il Tribunale, in composizione monocratica, , definitivamente pronunciando sulla domanda proposta, ogni contraria istanza ed eccezione disattesa, così provvede:

-rigetta le domande proposte dall'attore;

comepnsa le spese

Così deciso in Torre Annunziata,

Il Go

dott. Salvatore Nasti