



TRIBUNALE DI LECCE
- Seconda Sezione civile -

proc. n. [REDACTED] R.g.

Il giudice,

- letti gli atti del proc. n. [REDACTED] rg promosso ex art. 702 bis e ss. da [REDACTED] e [REDACTED] che esponevano:
 - di essere contitolari del conto corrente [REDACTED] presso l'istituto di credito [REDACTED] spa e di aver ricevuto, in data 23.3.2013, una e-mail con mittente l'indirizzo "[REDACTED]", avente ad oggetto una richiesta di controllo della propria posizione mediante accesso ad un link riportato in calce;
 - di avere effettuato l'accesso al conto corrente *online*, sia in data 23.3.2013 che il giorno successivo, digitando i codici identificativi personali, nonché nome utente e password, avendo attribuito la paternità della suddetta e-mail alla banca;
 - di essersi immediatamente avveduti che erano stati effettuati, senza autorizzazione alcuna da parte dei due intestatari, quattro versamenti di "ricarica internet carta", due dell'importo di € 3.000,00 e due di € 2.000,00, per la complessiva somma, quindi, di € 10.000,00;
 - di avere pertanto diritto al rimborso della suddetta somma, oltre interessi e rivalutazione dalla domanda, da parte del [REDACTED], essendo state vittime di frode informatica [cd. *phishing*], non avendo la banca apprestato strumenti e presidi di sicurezza idonei ad evitare l'accesso fraudolento di terzi ai depositi dei propri clienti - quali dispositivi automatici per la generazione di password (token, chiavette, digipass) - o, comunque, a neutralizzarne gli effetti, oltre al risarcimento del danno non patrimoniale, quantificato in € 9.000,00, per lesione della sfera di riservatezza, avendo l'istituto di credito fornito dati a terzi nonché per la sofferenza emotiva cagionata dalla situazione debitoria scaturitane;
- preso atto della posizione difensiva di replica di [REDACTED] che eccepiva:
 - la non imputabilità dell'accaduto all'intermediario bancario, avendo quest'ultimo dapprima condotto un'intensa campagna pubblicitaria volta ad informare la propria clientela in merito alle precauzioni da seguire ed in seguito apprestato ogni opportuno mezzo di garanzia antifrode, inviando, successivamente al primo valido accesso effettuato dai ricorrenti, i quali hanno spontaneamente fornito al malversatore i codici di accesso e dispositivi per i servizi di *home banking*, un primo sms recante le password temporanee per confermare la richiesta di variazione del numero telefonico ed un secondo sms recante un "alert" per il cambiamento del numero;
 - la esclusiva responsabilità dei clienti che hanno colposamente continuato ad interagire con il portale contraffatto vanificando gli apprestati presidi di sicurezza;
 - l'infondatezza, perciò, tanto della domanda di rimborso delle somme sottratte, non potendo essere mosso alcun addebito al convenuto istituto di credito, quanto della domanda risarcitoria, sprovvista di corredo probatorio alcuno in ordine all'effettivo danno patito;
- preso atto delle deduzioni formulate alla prima udienza del 17 luglio scorso ed in scioglimento della riserva ivi assunta;

osserva

la controversia attiene, come dedotto dalla stessa parte ricorrente, alla fattispecie criminosa denominata "*phishing*", che consiste in una truffa informatica realizzata

mediante l'invio di e-mail o sms al fine di carpire dal titolare di un conto corrente bancario le credenziali, i codici di accesso e le password temporanee di accesso al conto, senza perciò violazione alcuna dei sistemi di sicurezza dell'intermediario bancario.

A tale riguardo, molteplici e differenti si sono rivelate le pronunce dell'Arbitro Finanziario Bancario e della giurisprudenza di merito e di legittimità, avendo di recente la Suprema Corte precisato che *"in tema di responsabilità della banca 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 valutarci con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente"* [Cass. sez. I, sent. 3.2.2017 n. 2950].

Gli stessi giudici di legittimità si sono soffermati, nell'ambito della motivazione di detta pronuncia, richiamata dai ricorrenti a verbale dell'ultima udienza, sul tema della responsabilità contrattuale per inadempimento del debitore ex art. 1218 cod. civ., precisando, nello specifico, come incomba sulla banca l'onere di fornire la prova di essersi attivata per l'accertamento in positivo della riconducibilità delle operazioni al cliente, dovendo lo stesso intermediario altresì dimostrare di aver predisposto idonee misure atte a verificare l'effettiva attribuibilità delle operazioni allo stesso e che, nonostante ciò, il comportamento del correntista sia stato talmente incauto da vanificarne comunque la predisposizione.

Nel caso di specie, ritiene questo Tribunale che alcun addebito possa essere mosso all'istituto di credito convenuto, avendo quest'ultimo fornito abbondante prova sia in ordine all'adempimento di preventivi obblighi informativi e pubblicitari volti ad erudire i propri clienti in merito al fenomeno in questione ed alle opportune cautele da adottare, come risulta rispettivamente dall'estratto del portale istituzionale del gruppo ~~XXXXXXXXXX~~ prodotto dal convenuto [doc. 4 in fasc. banca] e dalla "Guida ai servizi via internet cellulare e telefono" presente sul sito internet della banca e a cui rimanda lo stesso contratto del 7.3.2012 nelle dichiarazioni conclusive a firma di ~~XXXXXXXXXX~~ [doc. n. 1 e 2 in fasc. banca], sia in ordine alla intervenuta predisposizione in concreto di presidi di sicurezza quali password temporanee ed sms di "alert" conseguenti alla richiesta di variazione del numero telefonico, più volte inviati al cliente e colposamente ignorati [doc. n. 9, ib.].

Avuto riguardo alla più dettagliata ricostruzione dei fatti fornita dalla banca convenuta, peraltro comprovata dal documento di tracciatura/operatività del conto corrente del ~~XXXXXXXXXX~~ e della ~~XXXXXXXXXX~~ [doc. n. 9 in fasc. parte convenuta], ricostruzione neppure contestata o smentita da questi ultimi, risulta come il correntista, in data 23.3.2013, dopo aver ricevuto una e-mail da ~~XXXXXXXXXX~~, caratterizzata, peraltro, da evidenti errori ortografici [doc. n. 3, in fasc. ricorrente], digitando su un link sospetto ed effettuando login valido, nonostante l'sms inviato dall'istituto di credito di avviso della anomala richiesta di variazione del numero telefonico oltre al successivo sms con "alert", abbia comunque persistito nel proprio incauto comportamento, inserendo altresì i codici temporanei fornitigli dal sistema di sicurezza bancario online.

Alla luce di quanto suesposto, risulta evidente come il cliente abbia colposamente violato gli obblighi di custodia sullo stesso gravanti tanto *ex contractu* quanto *ex lege* [art. 7 d.lgs. 11/2010, approvato in attuazione di direttiva 2007/64/CE "relativa ai servizi di

pagamento nel mercato interno"], non potendosi di conseguenza configurare alcun danno patrimoniale risarcibile, avendo lo stesso correntista spontaneamente fornito username, password e codici OTS/OTP temporanei, idonei a consentire l'accesso di terzi al proprio conto ed ai propri dati personali, e ciò nonostante i plurimi segnali di anomalia riscontrabili, che un correntista avveduto ed informato avrebbe già dovuto riconoscere, e gli avvertimenti inoltrati dalla banca, che anche un correntista non esperto non avrebbe dovuto ignorare.

Rigettata la domanda, quanto alle spese di procedura, le stesse vanno liquidate secondo soccombenza sulla scorta dei criteri previsti dal d.m. 55/14 ed in misura prossima ai minimi dei parametri previsti per i giudizi ordinari e sommari di cognizione di valore fino a 26 mila euro con riguardo alle fasi di studio, introduttiva e decisionale.

p.f.m.

rigetta il ricorso in premessa.

Condanna ~~_____~~ e ~~_____~~ a rifondere a ~~_____~~ spa le spese e competenze del presente giudizio, da liquidarsi in € 1.700,00 per compenso professionale, oltre spese a forfait al 15%, Cassa Avvocati ed Iva di legge.

Lecce, 11 ottobre 2018

Il giudice
dr. Paolo Moroni

Dep. 11.10.2018
11.10.2018