COLLEGIO DI NAPOLI – DECISIONE N. 2660/2017 – PRES.CARRIERO – REL.SANTAGATA

Conto corrente – bonifico transfrontaliero tramite *home banking* – disconoscimento - violazione degli obblighi di custodia in capo al ricorrente- responsabilità del prestatore dei servizi di pagamento – insussistenza (cod. civ., art. 2729; d. lgs. n. 11/2010, art. 7).

FATTO

La società ricorrente (omissis), espone che, in data 9.6.2016, in occasione di una verifica *on line* sul conto corrente a lei intestato, è risultatoche in data 10.5.2015 (omissis) ignoti avevano effettuato un bonifico estero nonautorizzato/fraudolento per euro 25.000,00 con causale "acconto per pratica", prontamentedenunciato alla Pubblica Autorità (allega denuncia al ricorso). La ricorrente precisa, al
riguardo, che: *a*) le credenziali di accesso al servizio di *internet banking*, ivi compreso ildispositivo *token,* sono da sempre in possesso del solo rappresentante legale della società e custoditi in luoghi soltanto allo stesso accessibili; *b*) gli accessi alla banca *on line* sono sempre stati effettuati da *PC* siti presso gli uffici amministrativi della società e copertida efficace antivirus; *c*) l'operazione fraudolenta è stata effettuata in giorno ed orario di lavoro, quando nella sede della società erano presenti sia il legale rappresentante che i dipendenti, per cui l'accesso al sistema deve essere avvenuto da un *computer* esterno.
Ciò premesso, riscontrato negativamente il reclamo, la società ricorrente (omissis), ha adito l'Arbitro al quale chiede la restituzione e/o rimborso della somma di euro 25.000,00 oltre interessi legali dalla data del reclamo e spese delpresente procedimento, ravvisando la responsabilità dell'intermediario per il bonifico non autorizzato/fraudolento per le seguenti ragioni: 1) il sistema di *internet banking* messo a disposizione della clientela non è dotato di un sistema di *sms alert* (offerto da tutti gli operatori) per avvisare l'utilizzatore dell'operazione fraudolenta; 2) la banca avrebbe dovuto accorgersi che il bonifico effettuato a favore di beneficiario straniero e per un importo di euro 25.000,00 era un'operazione quantomeno "dubbia", considerato che la società non ha mai effettuato bonifici a favore di beneficiari fuori dall'area Euro; 3) a differenza di quanto affermato dalla banca, l'adozione di OTP non garantisce la totale invulnerabilità del sistema, come confermato dalla Banca d'Italia nella "premessa" al provvedimento dell'11.2.2011 di attuazione del titolo II del D. Lgs. 11/2010.
Costituitosi ritualmente, l'intermediario chiede all'Arbitro di respingere il ricorso o – in subordine – di accertare un concorso di colpa nella produzione del danno lamentato dalla ricorrente, con compensazione delle spese di procedimento.
Al riguardo la banca ha eccepito che la ricorrente si è accorta del bonifico fraudolento ben 30 giorni dopo l'operazione, pur essendo una società che, come tale, presumibilmente controlla attentamente e di frequente la propria situazione finanziaria; ha inoltre precisato che: 1) adotta strumenti di sicurezza evoluti ed affidabili definiti come sistemi di autenticazione a "due fattori" (*token* o OTP) di "impossibile forzatura", coerenti con le indicazioni del provvedimento della Banca d'Italia adottato il 5 luglio 2011, e fornisce alla
clientela – via *internet* – precise indicazioni volte a sventare intrusioni informatiche offensive; 2) da un'analisi effettuata dal sistema informatico della banca non risulta compromessa la tecnologia e il bonifico risulta inviato da una sessione autentica dell'utente (quindi da persona che disponeva del *token*), che peraltro aveva chiesto di poter effettuare bonifici esteri indicando come importo massimo giornaliero euro 80,000,00; 3) in sede di sottoscrizione del contratto, la società ricorrente aveva preferito
non avvalersi del sistema di *sms alert* offerto a tutta la clientela.

DIRITTO

La fattispecie all'esame del Collegio verte sul disconoscimento di un'operazione di bonifico estero *on line* eseguito tramite il servizio di *home banking*.

Per la soluzione della controversia vengono in considerazione le disposizioni del d. lgs. 11/2010, il quale ha recepito la direttiva 2007/64/CE (PSD), relativa ai servizi di pagamento nel mercato interno europeo ed, in particolare: *a*) l'art. 10, secondo cui, in caso di disconoscimento di un'operazione di pagamento, "*è onere dell'intermediario dimostrare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema*"; *b*) l'art. 8, ove si dispone che "*Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di … 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 ai sensi dell'articolo 7 (…)*; *c*) l'art. 7, che obbliga l'"*utilizzatore abilitato all'utilizzo di uno strumento di pagamento"* a:
"*utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso"*; *"comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza"*; ed, infine, ad adottare "*le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo*".
Alla luce del quadro normativo testé indicato, al fine di stabilire l'eventuale responsabilità della banca per i danni derivanti da un'operazione fraudolenta occorre dunque verificare: per un verso, l'osservanza da parte del cliente degli obblighi circa la custodia e l'uso dei codici di accesso cui è astretto nell'utilizzo degli strumenti di pagamento e, per altro verso, il grado di diligenza che l'intermediario ha impiegato nell'erogazione del servizio di *home banking*.
Sennonché, costituisce orientamento ormai consolidato di questo Arbitro che la prova della colpa grave ha ad oggetto la dimostrazione dei fatti che, in connessione tra loro, possono ragionevolmente condurre a ritenere gravemente negligente la condotta del cliente. In particolare, l'onere della prova da parte dell'intermediario – che non ha accesso ad informazioni relative all'organizzazione dei propri clienti ed alle modalità di custodia dei citati dispositivi ulteriori rispetto a quelle dichiarate dai clienti stessi in sede di denuncia e di reclamo – può essere assolto soltanto ed esclusivamente mediante un insieme di elementi gravi, precisi e concordanti (art. 2729 c.c.) dai quali possa desumersi la sussistenza di comportamenti negligenti da parte dell'utilizzatore (così ABF Napoli, dec.nn. 1033/2012; 2179/2016; 11189/2016).
Ebbene, nel caso di specie il Collegio ritiene sussistere tale serie univoca e concordante di elementi atti a dimostrare la negligenza del ricorrente. Ed invero, da un lato l'esecuzione del bonifico implica la disponibilità del *token*, il quale – secondo quanto affermato dalla ricorrente – è sempre rimasto nella sua disponibilità, sicché è ravvisabile una violazione dell'obbligo di custodia dello strumento di pagamento prescritto dall'art. 7, comma 1, lett. *a*), d.lgs. n. 11/2010.
Dall'altro lato, dall'esame dei documenti e dei *"log*" prodotti dall'intermediario, il Collegio reputa adeguatamente provato che il sistema informatico dell'intermediario sia rimasto integro ed abbia correttamente funzionato. Ciò in quanto: 1) è certo, e risulta dal tracciato degli accessi dell'*home banking* prodotto dalla banca convenuta, che la ricorrente abbia immesso nel sistema le sue credenziali protette e le sue *password* OTP; 2) l'intermediario risulta aver assolto agli obblighi di sicurezza posti a suo carico dotando il cliente di un sistema *one time password* e quindi di un sistema di autenticazione a due fattori caratterizzato notoriamente da elevata capacità protettiva; 3) l'intermediario ha altresì reso disponibile il servizio di *sms alert*, al quale la ricorrente ha scelto di non aderire.
Peraltro, nella specie non possono neppure ravvisarsi gli estremi di un comportamento negligente dell'intermediario per avere consentito l'esecuzione di un bonifico "insolito", in quanto vi è documentazione in atti, per giunta relativa al medesimo contesto temporale del bonifico contestato, sia relativa altro bonifico estero di importo maggiore a quello oggetto di

doglianza (euro 42.385,45 in data 6 aprile 2016), sia della richiesta della ricorrente di elevazione del massimale giornaliero per bonifici esteri da euro 50.000,00 ad euro 80.000,00 (in data 19 febbraio 2016)**.**

Alla luce del quadro fattuale innanzi esposto, è sicuramente applicabile alla specie il costante orientamento dell'Arbitro secondo cui "*l'adozione di un sistema a "due fattori"induce a ritenere, in assenza di ulteriori indici di anomalia dell'operazione, da un lato, che*
la banca abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del d.lgs. n. 11/2010 (in questo senso Coll. Milano, dec.6309/2013, dec. 1458/2015) e, dall'altro lato, che il cliente si sia reso gravemente inadempiente all'obbligo di custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio online e l'invio di ordini di bonifico a valere sul conto a lui intestato. Si tratta delle metodologie che, allo stato, appaiono più avanzate per proteggere la clientela rispetto ai rischi connessi all'effettuazione di operazioni on line. L'adozione di questi dispositivi è in linea con le indicazioni fornite dalla Banca d'Italia nel Provvedimento del 5 luglio 2011".

È dunque lecito presumere che l'operazione fraudolenta di cui si discute sia stata resa possibile da un comportamento inadempiente del cliente, il quale ha omesso di adottare tutte le cautele necessarie a custodire i codici di accesso e i dispositivi connessi e, pertanto, il ricorso non può quindi essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.