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

**ente – bonifico transfrontaliero tramite *home banking* – disconoscimento - violazione degli obblighi di
icorrente- responsabilità del prestatore dei servizi di pagamento – insussistenza (**cod. civ., art. 2729; d.
t. 7).

FATTO

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

DIRITTO

ie all'esame del Collegio verte sul disconoscimento di un'operazione di bonifico estero *on line* eseguito tramit
nking.
zione della controversia vengono in considerazione le disposizioni del d. lgs. 11/2010, il quale ha recepito
(PSD), relativa ai servizi di pagamento nel mercato interno europeo ed, in particolare: *a*) l'art. 10, secondo cui
cimento di un'operazione di pagamento, "*è onere dell'intermediario dimostrare che l'operazione sia stata co
registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive
nti del sistema*"; *b*) l'art. 8, ove si dispone che "*Il prestatore di servizi di pagamento che emette uno s
ha l'obbligo di … assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagam
ssibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi pos
ai sensi dell'articolo 7 (…)*; *c*) l'art. 7, che obbliga l'"*utilizzatore abilitato all'utilizzo di uno strumento di pagame
strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissio
e senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al s
ndicato, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena
*"; ed, infine, ad adottare "*le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consen

el quadro normativo testé indicato, al fine di stabilire l'eventuale responsabilità della banca per i danni c
ne fraudolenta occorre dunque verificare: per un verso, l'osservanza da parte del cliente degli obblighi circa la
odici di accesso cui è astretto nell'utilizzo degli strumenti di pagamento e, per altro verso, il grado di di

bia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del d.lgs. n.
so Coll. Milano, dec.6309/2013, dec. 1458/2015) e, dall'altro lato, che il cliente si sia reso gravemente in
li custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio online e l'invio di ordini
onto a lui intestato. Si tratta delle metodologie che, allo stato, appaiono più avanzate per proteggere la clientel
essi all'effettuazione di operazioni on line. L'adozione di questi dispositivi è in linea con le indicazioni fornite
Provvedimento del 5 luglio 2011".

ecito presumere che l'operazione fraudolenta di cui si discute sia stata resa possibile da un comportamento in
il quale ha omesso di adottare tutte le cautele necessarie a custodire i codici di accesso e i dispositivi
ricorso non può quindi essere accolto.

P.Q.M.

non accoglie il ricorso.