

La responsabilità contrattuale della banca nel phishing

di AVV. MARIA TERESA DE LUCA

Il Tribunale di Gela con l'ordinanza depositata il 23 luglio 2021¹, torna ad occuparsi di una vicenda di frode online, c.d. phishing.

1. BREVI CENNI SUL PHISHING

In ambito informatico il *phishing* ("pesca" - di dati sensibili) è un'attività illegale rivolta a ottenere l'**accesso a informazioni personali o riservate con la finalità del furto di identità** tramite l'invio di **e-mail**, con mittenti autorevoli e reali e contenuti verosimili, con l'invito ad accedere a falsi siti che imitano la grafica dei siti istituzionali per ottenere informazioni come la password di accesso ai servizi online o al conto corrente, oppure il numero della carta di credito. Se è vero che utilizzare i servizi di home banking consente di accedere e gestire i nostri conti correnti con estrema facilità, queste procedure allo stesso tempo espongono l'utente della banca al rischio elevato di truffe online attraverso il phishing.

Di solito, l'attività del phisher inizia con l'invio di un messaggio di posta elettronica alla vittima. Il messaggio proviene a prima vista da banche, istituti finanziari, società erogatrici di servizi, da agenzie governative o siti web e avvisa la vittima di un problema che è stato riscontrato su queste piattaforme. Per risolvere il problema, la vittima viene, pertanto, invitata a visitare la pagina internet del servizio, attraverso un apposito link inviato con l'e-mail. Se il malcapitato utente clicca sul link, viene rinvio a una pagina Web che, riproducendo perfettamente quella originale del servizio utilizzato, lo determina a digitare le proprie credenziali di accesso al

servizio. E se l'utente inserisce lo username e la password nella finta pagina Web, la truffa online si è praticamente realizzata, in quanto i dati saranno ormai nella disponibilità dei cyber criminali, che li utilizzeranno per accedere ai profili realmente controllati dalla vittima.

Ma questa su descritta è solo una delle diverse varianti di truffa online.

Infatti, le **tecniche** usate dai **cybercriminali** si fanno sempre più sofisticate e mescolano **elementi tecnologici e ingegneria sociale**.

I criminali del web hanno, infatti, progettato e affinato le più variegata tecniche per ottenere accesso ai dati delle carte di credito o dell'home banking del malcapitato di turno. Ed ecco che al **phishing** "tradizionale", tramite e-mail, si aggiunge lo **smishing**, dove il messaggio fraudolento è inviato tramite SMS, o il **caller ID spoofing**, che consiste nel mascherare il numero del chiamante facendolo apparire come il numero verde di un istituto bancario, in modo da carpire la buona fede della vittima che si fida e comunica le proprie credenziali di autenticazione. Esiste poi, il **SIM Swapping** che rappresenta una particolare tipologia di truffa con cui il criminale del web dichiara falsamente, contattando o recandosi in un centro assistenza, di aver smarrito o subito il furto del telefono cellulare. Il truffatore chiede al centro di assistenza di disabilitare la vecchia scheda SIM per ottenerne una nuova con lo stesso numero, appropriandosi, di fatto, del numero di telefono della vittima. Questa tecnica è particolarmente

Note:

1) Si allega a pagina 55 la Sentenza.

efficace se abbinata con il possesso delle credenziali di accesso dell'home banking della vittima. In questo modo è infatti possibile aggirare anche i sistemi di autenticazione a due step basati sull'invio di SMS con **One Time Password** da parte degli istituti bancari per autorizzare le transazioni. La vittima di SIM Swap osserverà semplicemente la perdita di segnale sul pro-prio telefono cellulare, causata dalla disattivazione della sua SIM originale, mentre il criminale rice-verà sulla nuova SIM clonata le OTP per eseguire le operazioni desiderate.

2. IL CASO

Un cliente propone reclamo ex art. 669-terdercies c.p.c. nei confronti della Banca, avverso l'ordinanza del Tribunale, che era stata emessa a definizione del giudizio ex art. 700 c.p.c., contestando sia il rigetto del suo ricorso per mancanza del *fumus boni iuris*, sia la condanna alle spese di lite.

Nella specie il cliente, titolare di un conto corrente, subisce una truffa informatica (cd. phishing), avente ad oggetto n. 21 operazioni bancarie *on line* (di cui: n. 20 operazioni di ricarica di carte pre-pagate di terzi dell'importo di € 2.499,00 ciascuna e n. 1 bonifico in favore di un terzo dell'importo di € 24.000,00) per la somma complessiva di

€ 73.980,00 di cui la somma di € 22.998,80 è stata riaccredita sul suo conto dalla banca, previo recupero tramite procedure interbancarie a seguito della sua segnalazione della truffa subita e agisce in giudizio per il riaccredito della ulteriore somma.

I motivi di ricorso: la responsabilità contrattuale della banca in ipotesi di phishing.

Preliminarmente il Tribunale richiama le disposizioni in materia di uso fraudolento dei sistemi di pagamento e dovere di diligenza dell'utilizzatore di cui agli **artt. 7 e 12 D. Lgs. n. 11 del 27 gennaio 2010** (Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, re-cante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE", nel testo vigente alla data di effettuazione delle operazioni bancarie riferite

al caso in esame)

Art. 7. Obblighi a carico dell'utilizzatore dei servizi di pagamento in relazione agli strumenti di pagamento: "1. L'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso; b) 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; 2. Ai fini di cui al comma 1, lettera a), l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo.

Art. 12. Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento: "1. Salvo il caso in cui abbia agito in modo fraudolento, l'utilizzatore non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b);

2. Salvo il caso in cui abbia agito in modo fraudolento, l'utilizzatore non è responsabile delle perdite derivanti dall'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo di cui all'articolo 8, com-ma 1, lettera;

3. Salvo il caso in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento, prima della comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b), l'utilizzatore medesimo può sopportare per un importo comunque non superiore complessivamente a 150 euro la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto o smarrimento.

In particolare, nel caso di specie assume carattere dirimente della controversia, secondo

il Tribunale, proprio il su citato art. 7, nella parte in cui prevede al comma 1, lett. a), che *“L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso”, con la precisazione di cui al comma 2 che “Ai fini di cui al comma 1, lettera a), l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurez-za personalizzate”, in combinato disposto con l'art. 12, nella parte in cui prevede al comma 4 che “Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'ar-ticolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamen-to non autorizzate e non si applica il limite di 50 € di cui al comma 3”.*

Sul piano delle condizioni contrattuali pattuite dalle parti, di cui al citato art. 7, comma 1, lett. a), d.lgs. n. 11/2010, il contratto stipulato dalle parti in causa relativo ai *“servizi via internet, cellulare e telefono”* afferenti al conto corrente per cui è causa, prevede all'art. 5 che *“1. Il Cliente riconosce a sé riferibili tutte le operazioni effettuate previo utilizzo dei codici, secondo quanto indicato nella Guida ai servizi. 2. Il Cliente prende atto che attraverso l'utilizzo dei codici è possibile disporre con effetto immediato dei beni e valori oggetto dei rapporti collegati. Pertanto, il Cliente si impegna a mantenere segreti i codici, che sono strettamente personali e non cedibili a terzi, nonché a custodirli e utilizzarli con la massima diligenza.”*, nonché la *“Guida ai Servizi”* a cui la suddetta clausola contrattuale rinvia, nella parte relativa ai *“consigli per la sicurezza”*, in cui prevede che *“i codici di identificazione sono strettamente personali: non devono essere assolutamente divulgati a terze persone e vanno custoditi separatamente”; “Non comunicare a nessuno i codici, in quanto le nostre politiche di sicurezza non prevedono la richiesta al cliente di fornire i suoi codici di accesso via e-mail o telefonicamente”.*

Nel caso *de quo* è stato accertato che le operazioni incriminate sono state eseguite dalla banca, in quanto il cliente, come da lui stesso dedotto, ha fornito al telefono ad un sedicente operatore

della banca stessa sia il codice OTP sia il codice OTS ricevuti al suo numero di cellulare indicato per il servizio di *home banking*, necessari per la conferma di ciascuna di tali operazioni.

Tale comportamento del correntista, come aveva correttamente ritenuto anche il Giudice *a quo*, integra un **inadempimento degli obblighi contrattualmente assunti** ai sensi dell'art. 5 del contratto, connotato da **colpa grave**, data la sua reiterazione per ben 21 operazioni e per ben 42 codici di conferma ad esse correlate, che come tale implica che il correntista sopporti tutte le perdite derivanti da tali operazioni di pagamento, ai sensi del citato combinato disposto dell'art. 7, comma 1, lett. a), e dell'art. 12, comma 4, del d.lgs. n. 11/2010, nel testo vigente alla data di effettuazione delle operazioni bancarie per cui è causa.

3. IL CORRETTO RIPARTO DELL'ONERE DELLA PROVA NEL GIUDIZIO PER PHISHING

Nel caso di specie, in base alle tracciate delle operazioni svolte sul portale home banking della banca resistente il giorno della frode dedotta è possibile ricostruire con certezza i fatti svoltisi e del resto, parte ricorrente non ha contestato né che tale documento rappresenti la verità degli accadimenti, né i fatti specificamente allegati dalla banca resistente.

Contrariamente a quanto dedotto dal cliente, non rileva che egli fosse convinto di relazionarsi al telefono con un operatore della banca resistente in quanto, come espressamente previsto dalle richia-mate condizioni contrattuali, i suddetti codici sono strettamente personali e servono al correntista per effettuare operazioni bancarie sul conto

on line in piena autonomia, senza l'intervento degli operatori bancari, che come tale avrebbe dovuto essere escluso dal correntista, secondo ordinaria diligenza, in base alla natura stessa delle operazioni bancarie che stava effettuando, oltre che in ossequio a quanto espressamente previsto e precisato dalle condizioni contrattuali pattuite.

4. L'OBLIGO DI CUSTODIA DEI CODICI DISPOSITIVI DEL PROPRIO CONTO

L'operazione abusiva contestata, in definitiva,

è stata resa possibile dal comportamento del ricorrente che ha violato **l'obbligo di custodia dei codici dispositivi del proprio conto**, utilizzandoli al di fuori del circuito operativo dell'intermediario e con modalità differenti da quelle stabilite, ovvero comunicandole ad un operatore, non previamente contattato, per via telefonica.

Pertanto, non sussiste alcuna responsabilità della banca resistente sia perché in base al combinato disposto dell'art. 7, comma 1, lett. a), e dell'art. 12, comma 4, del d.lgs. n. 11/2010, l'accertata colpa grave del correntista nell'impiego dei strumenti e dei servizi di pagamento implica la sopportazione a suo carico delle perdite derivanti da operazioni non autorizzate, sia perché la banca ha ottemperato all'obbligo di cui all'art. 8, comma 1, lett. d), d.lgs. n. 11/2010, a seguito della sua comunicazione ex art. 7, comma 1, lett. b) d.lgs. n. 11/2010, da lui effettuata tuttavia solo dopo l'esecuzione di tutte le operazioni bancarie, come dallo stesso dichiarato in sede di denuncia alla Stazione dei Carabinieri di Gela, sicché il recupero delle somme è stato possibile, grazie all'intervento della banca, nei limiti del consenso alla restituzione prestato da uno dei beneficiari e della disponibilità presente sul suo conto, per l'importo di € 22.998,80.

Pertanto, il correntista non ha diritto al riaccredito da parte della banca dell'ulteriore somma residua, a fronte della somma complessiva di € 73.980,00 oggetto delle operazioni per cui è causa, in quanto la perdita residua subita è imputabile esclusivamente al suo inadempimento, connotato da colpa grave, degli obblighi contrattuali su di lui gravanti nell'uso degli strumenti e dei servizi di pagamento inerenti al contratto di *home banking* stipulato con l'istituto di credito.

Il reclamo è stato rigettato e, per l'effetto, è stata confermata l'ordinanza impugnata del Presidente del Tribunale, emessa a definizione del giudizio ex art. 700 c.p.c..

In conclusione:

- **tutte le operazioni di pagamento impartite sul conto del ricorrente sono state autenticate regolarmente mediante i codici forniti;**
- **non vi è stata alcuna anomalia nel sistema di sicurezza della Banca la quale ha assolto**

l'onere di provare l'adempimento degli obblighi su di essa gravanti;

- **il cliente si è reso gravemente inadempiente rispetto all'obbligo di custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio online.**

5. L'ORIENTAMENTO DELLA GIURISPRUDENZA E DELL'ABF

Del resto, la giurisprudenza è concorde nel ritenere che la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, avendo natura contrattuale, è esclusa se ricorre colpa grave dell'utente e che rientra nel rischio tipico 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 (cfr. Cassazione civile sez. III, 05/07/2019, n.18045: *"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, configurabile nel caso di protratta mancata attivazione di una qualsiasi forma di controllo degli estratti conto"* e Cassazione civile, sez. I, 03/02/2017, n. 2950: *"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 valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente").

Si sottolinea che in una recente decisione l'Arbitro Bancario Finanziario (n. 17200 del 19.7.2021) richiama in caso di phishing, altresì le Disposizioni della Banca d'Italia del 5.7.2011 emanate in "Attuazione del Titolo II del D.lgs. n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento", ove vengono meglio precisati gli obblighi di custodia dei dispositivi di sicurezza in capo all'utilizzatore e la responsabilità derivante dalla mancata osservanza degli stessi. Sez. IV, Paragrafo 2.1 (Riservatezza dei dispositivi di sicurezza): *"Quando uno strumento prevede l'utilizzo di dispositivi personalizzati di sicurezza (es. PIN e password) è fatto obbligo all'utilizzatore di mettere in atto gli accorgimenti idonei al fine di preservarne la riservatezza onde evitare gli utilizzi non autorizzati degli strumenti di pagamento in questione. Tale esigenza rileva in modo specifico nel caso in cui il pagamento sia effettuato a distanza, ad esempio per mezzo di un dispositivo telefonico o di un sito internet. E' necessario che l'utilizzatore ottenga l'autorizzazione del proprio prestatore di servizi di pagamento prima di fornire a terzi i codici per l'utilizzo del servizio o dello strumento di pagamento: in tal modo è possibile per il prestatore individuare le richieste dei codici di sicurezza provenienti da soggetti che simulino la legittimità della richiesta medesima, come nel caso del phishing. In aggiunta, ciò consente di limitare i rischi connessi con l'eventuale utilizzo di piattaforme per i pagamenti su internet (in particolare quelli a valere su un conto, quali i bonifici) che non sono autorizzate dal prestatore di servizi di pagamento di cui l'utilizzatore si avvale (cc.dd. overlay services). Qualora il contratto tra utilizzatore e prestatore di servizi di pagamento faccia divieto al primo di comunicare a terzi i codici di sicurezza, la violazione di tale divieto integra una condotta negligente da parte dell'utilizzatore, non*

consentendogli di avvalersi dell'esenzione di responsabilità di cui al successivo paragrafo". Paragrafo 2.2 (Responsabilità dell'utilizzatore): *"Il rispetto degli obblighi di condotta diligente da parte dell'utilizzatore esime quest'ultimo da responsabilità per utilizzi non autorizzati dei servizi e degli strumenti di pagamento. Il mancato adempimento di tali obblighi può invece comportare la sua responsabilità per gli utilizzi non autorizzati. La violazione degli obblighi posti in capo all'utilizzatore dalla legge o dal contratto in essere con il suo prestatore di servizi di pagamento integra una condotta negligente. Al fine di favorire la diffusione dei servizi e degli strumenti di più elevata qualità sotto il profilo della sicurezza, la Banca d'Italia, ai sensi dell'art. 12, comma 5, del Decreto, dispone la riduzione delle responsabilità dell'utilizzatore che scelga detti prodotti di pagamento. Rientrano nella fattispecie in esame gli strumenti di pagamento aventi le caratteristiche di sicurezza individuate nel documento "Tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza" allegato al presente Provvedimento. Per questi strumenti - fatti salvi i casi in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento - l'utilizzatore non risponde neppure della franchigia di cui all'art. 12, comma 3, del Decreto".* Il Collegio di Coordinamento, con decisione n. 22745/2019, ha inoltre enunciato il seguente principio di diritto: *"la previsione di cui all'art. 10, comma 2, del d.lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente".*

N. 729/2021 R.G.



Tribunale Ordinario di Gela

SEZIONE CIVILE

Riunito in camera di consiglio, nelle persone dei seguenti magistrati:

dott.ssa Maria Rosaria Carlà	Presidente
dott.ssa Stefania Sgroi	Giudice rel. estens.
dott. Vincenzo Accardo	Giudice

a scioglimento della riserva assunta all'udienza collegiale del 13/07/2021;

ha emesso la seguente

ORDINANZA

nel procedimento per reclamo iscritto al n. 729/2021 R.G.

promosso da

(c.f.), con il ministero degli avv.ti e

reclamante

contro

(p.i.) in persona del rappresentante legale p.t., con il ministero dell'avv.

reclamata

1. ha ritualmente proposto reclamo ex art. 669-terdecies c.p.c. nei confronti della banca s.p.a. in persona del rappresentante legale p.t., ritualmente costituitasi, avverso l'ordinanza n. 264/2021 del presente Tribunale, emessa a definizione del giudizio ex art. 700 c.p.c. iscritto al n. 342/2021 R.G., contestando sia il rigetto del suo ricorso per mancanza del *fumus boni iuris*, sia la condanna alle spese di lite.

2. Il reclamo è infondato per le ragioni che seguono.

2.1. Il primo motivo di reclamo, con cui si contesta la mancanza del *fumus boni iuris* del ricorso ritenuta dal Giudice *a quo*, è infondato tenuto conto del quadro normativo di riferimento e delle risultanze istruttorie, come correttamente considerati dal Giudice *a quo*.

In particolare, risulta in atti che è titolare del c/c n. presso la filiale della banca s.p.a. sita a in via , in relazione al quale in data 22.09.2020 ha subito una truffa informatica (cd. phishing), avente ad

oggetto n. 21 operazioni bancarie *on line* (di cui: n. 20 operazioni di ricarica di carte prepagate di terzi dell'importo di € 2.499,00 ciascuna e n. 1 bonifico in favore di un terzo dell'importo di € 24.000,00) per la somma complessiva di € 73.980,00 di cui la somma di € 22.998,80 è stata riaccredita sul suo conto dalla banca, previo recupero tramite procedure interbancarie a seguito della sua segnalazione della truffa subita; agisce in giudizio per il riaccredito della ulteriore somma.

Come correttamente ritenuto dal Giudice *a quo*, nel caso di specie trova applicazione il d.lgs. n. 11/2010, recante la *“Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE”*, nel testo vigente alla data di effettuazione delle operazioni bancarie per cui è causa (22.09.2020).

In particolare, nel caso di specie assume carattere dirimente della controversia alla luce delle risultanze istruttorie, l'art. 7, rubricato *“Obblighi a carico dell'utente dei servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate”*, nella parte in cui prevede al comma 1, lett. a), che *“L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso”*, con la precisazione di cui al comma 2 che *“Ai fini di cui al comma 1, lettera a), l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate”*, in combinato disposto con l'art. 12, rubricato *“Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento”*, nella parte in cui prevede al comma 4 che *“Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 € di cui al comma 3”*.

Sul piano delle condizioni contrattuali pattuite dalle parti, di cui al citato art. 7, comma 1, lett. a), d.lgs. n. 11/2010, va considerato il contratto n. stipulato dalle parti in causa il 31.01.2012 relativo ai *“servizi via internet, cellulare e telefono”* afferenti al conto corrente per cui è causa, nella parte in cui prevede all'art. 5 che *“1. Il Cliente riconosce a sé riferibili tutte le operazioni effettuate previo utilizzo dei codici, secondo quanto indicato nella Guida ai servizi. 2. Il Cliente prende atto che attraverso l'utilizzo dei codici è possibile disporre con effetto immediato dei beni e valori oggetto dei rapporti collegati. Pertanto, il Cliente si impegna a mantenere segreti i codici, che sono strettamente personali e non cedibili a terzi, nonché a custodirli e utilizzarli con la massima diligenza.”* (v. all. 6, fasc. banca di 1° grado), nonché la *“Guida ai Servizi”* a cui la suddetta clausola contrattuale rinvia, nella parte relativa ai *“consigli per la sicurezza”*, in cui prevede che *“i codici di identificazione sono strettamente personali: non devono essere assolutamente divulgati a terze persone e vanno custoditi separatamente”*; *“Non comunicare a nessuno i codici, in quanto le*

nostre politiche di sicurezza non prevedono la richiesta al cliente di fornire i suoi codici di accesso via e-mail o telefonicamente” (v. all. 4, fasc. banca di 1°grado).

Nel caso di specie è stato accertato che le operazioni per cui è causa sono state eseguite dalla banca, in quanto T., come da lui stesso dedotto, ha fornito al telefono ad un sedicente operatore della banca stessa sia il codice OTP sia il codice OTS ricevuti al suo numero di cellulare indicato per il servizio di *home banking*, necessari per la conferma di ciascuna di tali operazioni.

Tale comportamento del correntista, come correttamente ritenuto dal Giudice *a quo*, integra un inadempimento degli obblighi contrattualmente assunti ai sensi dell’art. 5 del contratto, connotato da colpa grave, data la sua reiterazione per ben 21 operazioni e per ben 42 codici di conferma ad esse correlate (v. all. 8, fasc. banca di 1°grado), che come tale implica che il correntista sopporti tutte le perdite derivanti da tali operazioni di pagamento, ai sensi del citato combinato disposto dell’art. 7, comma 1, lett. a), e dell’art. 12, comma 4, del d.lgs. n. 11/2010, nel testo vigente alla data di effettuazione delle operazioni bancarie per cui è causa (22.09.2020).

Contrariamente a quanto dedotto dal reclamante, non rileva che egli fosse convinto di relazionarsi al telefono con un operatore della banca resistente in quanto, come espressamente previsto dalle richiamate condizioni contrattuali, i suddetti codici sono strettamente personali e servono al correntista per effettuare operazioni bancarie sul conto *on line* in piena autonomia, senza l’intervento degli operatori bancari, che come tale avrebbe dovuto essere escluso dal correntista, secondo ordinaria diligenza, in base alla natura stessa delle operazioni bancarie che stava effettuando, oltre che in ossequio a quanto espressamente previsto e precisato dalle condizioni contrattuali pattuite.

Contrariamente a quanto dedotto dal reclamante, non sussiste alcuna responsabilità della banca resistente sia perché in base al combinato disposto dell’art. 7, comma 1, lett. a), e dell’art. 12, comma 4, del d.lgs. n. 11/2010, l’accertata colpa grave del correntista nell’impiego dei strumenti e dei servizi di pagamento implica la sopportazione a suo carico delle perdite derivanti da operazioni non autorizzate, sia perché la banca ha ottemperato all’obbligo di cui all’art. 8, comma 1, lett. d), d.lgs. n. 11/2010, a seguito della sua comunicazione ex art. 7, comma 1, lett. b) d.lgs. n. 11/2010, da lui effettuata tuttavia solo dopo l’esecuzione di tutte le operazioni bancarie per cui è causa, come da lui stesso dichiarato in sede di denuncia alla Stazione dei Carabinieri di Gela (v. all. 1, ricorso), sicché il recupero delle somme è stato possibile, grazie all’intervento della banca, nei limiti del consenso alla restituzione prestato da uno dei beneficiari e della disponibilità presente sul suo conto, per l’importo di € 22.998,80.

Pertanto, il correntista non ha diritto al riaccredito da parte della banca dell’ulteriore somma residua, a fronte della somma complessiva di € 73.980,00 oggetto delle operazioni per cui è causa, in quanto la perdita residua subita è imputabile esclusivamente al suo inadempimento, connotato da

colpa grave, degli obblighi contrattuali su di lui gravanti nell'uso degli strumenti e dei servizi di pagamento inerenti al contratto di *home banking* stipulato il 31.01.2012.

2.2. Il secondo motivo di reclamo, afferente alla condanna alle spese di lite, è anch'esso infondato, in quanto il Giudice *a quo* ha correttamente condannato il ricorrente per soccombenza (art. 91 c.p.c.), data la mancanza del *fumus boni iuris* del ricorso ex art. 700 c.p.c. da lui proposto, tenendo conto altresì, in sede di quantificazione ex d.m. n. 55/2014 come aggiornato dal d.m. n. 37/2018, della semplicità della controversia, data la sua natura documentale, con conseguente riduzione al 50% ex art. 4, co.1, d.m. cit.

3. Alla luce delle superiori considerazioni, il reclamo va rigettato e, per l'effetto, l'ordinanza reclamata va confermata.

Le spese del presente giudizio di reclamo seguono la soccombenza e sono liquidate nella misura indicata in dispositivo ex d.m. n. 55/2014 come aggiornato dal d.m. n. 37/2018, tenendo conto della natura della causa (procedimento cautelare), del valore della causa come da domanda (€ 49.980,00) e delle fasi processuali espletate (3 fasi con esclusione della fase istruttoria, di bassa complessità, data la natura documentale della causa trattata in unica udienza, da liquidarsi ai medi ridotti del 50% ex art. 4, co.1, d.m. cit.,).

Si dà atto della sussistenza dei presupposti per il versamento, da parte del reclamante, dell'ulteriore importo a titolo di contributo unificato pari a quello dovuto per la stessa impugnazione ai sensi dell'art. 13, co. 1-quater, D.P.R. n. 115/2002.

P.Q.M.

rigetta il reclamo e, per l'effetto, conferma l'ordinanza impugnata n. 264/2021 del presente Tribunale, emessa a definizione del giudizio ex art. 700 c.p.c. iscritto al n. 342/2021 R.G.; condanna a pagare a S.P.A. (p.i.) in persona del rappresentante legale p.t. le spese del presente giudizio, liquidandole in € 1.822,50 per compenso, oltre spese generali al 15%, i.v.a. e c.p.a. nella misura di legge;

dà atto della sussistenza dei presupposti per il versamento, da parte del reclamante dell'ulteriore importo a titolo di contributo unificato pari a quello dovuto per la stessa impugnazione ai sensi dell'art. 13, co. 1-quater, D.P.R. n. 115/2002. Così deciso nella camera di consiglio del 23/07/2021.

IL GIUDICE REL. ESTENS.

dott.ssa Stefania Sgroi

IL PRESIDENTE

dott.ssa Maria Rosaria Carlà