COLLEGIO DI BOLOGNA – DEC.13280/2022 – PRES. MARINARI – REL. LUCARELLI

Strumenti di pagamento – home banking- frode informatica – responsabilità dell'intermediario (d.m. n. 112/2007, art. 8; d.lgs. n. 11/2010, art. 10).

Quando nel computer del cliente venga scaricato uno specifico malware (c.d. man in the browser, di difficile identificabilità e particolarmente insidioso) per l'esecuzione fraudolenta di operazioni di home banking, viene esclusa la colpa grave del cliente sempreché il computer sia stato dotato di un adeguato programma di antivirus. **(MDC).**

FATTO

Parte ricorrente, titolare del conto corrente n. **20 presso l'intermediario resistente, riferisce che in data 25.09.2018 la propria segretaria accedeva all'area riservata del sito del resistente per eseguire un bonifico, aprendo un sito identico al sito originale dell'intermediario perché avente apparentemente la stessa url, stesso logo, stessa impostazione grafica, stessi caratteri e maschera apparentemente identica, all'interno del quale seguiva la procedura prevista e inseriva i codici richiesti; il primo tentativo di bonifico non andava a buon fine; dopo pochi minuti, al secondo tentativo di accesso, veniva richiesto un codice OTP temporaneo, generato dal token, al fine di validare l'operazione di bonifico richiesta; subito dopo aver digitato il codice OTP, compariva improvvisamente la scritta "sito in manutenzione". Il giorno successivo, 26.09.2018, la segretaria, riuscendo finalmente ad accedere al sistema home banking per eseguire il predetto bonifico, apprendeva che ignoti avevano disposto dal conto un bonifico estero di importo pari a €
42.500,53; l'operazione veniva prontamente disconosciuta tramite raccomandata del 01.10.2018 e, dopo numerose richieste di riscontro, in data 22.04.2021 veniva inoltrato all'intermediario un formale reclamo, prospettando la frode subita come una tipologia particolarmente insidiosa, altresì nota come "man in the browser". Il riscontro tardivo al reclamo negava la disponibilità di un rimborso della somma richiesta; tale diniego era già pervenuto da parte del resistente, a seguito di precedente istanza di mediazione e al conseguente verbale negativo di adesione del 21.01.2019. La complessa frode conosciuta come "man in the browser" è descritta nella relazione peritale allegata al ricorso: l'esecuzione all'interno del browser di un codice malevolo che spia il comportamento dell'utente e raccoglie i suoi dati personali, inclusi gli account di home banking, ha un impatto sull'usabilità del browser, poiché lo rende certamente più lento e interferisce con l'attività dell'utente, come del resto è stato percepito per tutta la giornata del 25.09.2018; la circostanza che l'IP della società sia rimasto sempre immutato, in quanto durante e dopo la frode questo corrispondeva all'IP ***188, unitamente ad altre circostanze descritte nella relazione tecnica, dal bonifico non andato a buon fine a tutti gli elementi estremamente rilevanti, dimostrano chiaramente che la frode realizzata a danno della vittima sia stato un attacco di "man in the browser". Secondo la parte istante, i rifermenti temporali delle operazioni di accesso e quelli relativi agli SMS ricevuti non sono allineati ed il sistema informatico dell'utente era adeguatamente protetto con software antivirus. Sempre secondo la parte istante, una delle carenze più evidenti del sistema del resistente era all'epoca dei fatti caratterizzata dalla mancanza di una notifica all'utente tramite email alert al semplice accesso o allo storico delle movimentazioni del conto corrente, oltre all'assenza di un

sistema di invio di e-mail o sms di alert per le singole operazioni bancarie dispositive. Il bonifico risulterebbe disposto intorno alle 9:45 del 25.09.2018 con la modalità "urgente" e anche se nel documento informativo consegnato al cliente non viene specificato l'orario limite per la revoca dei bonifici. Il ricorrente afferma che dalla relazione tecnica redatta emerge che sul PC utilizzato per l'internet banking oggetto della frode è stata rilevata la presenza di un malware, il Trojan DXXX, identificato dall'antivirus, scaricato il giorno prima dell'operazione disconosciuta come allegato di un messaggio posta elettronica; i malintenzionati tramite questo malware introdotto nel sistema informatico della società ricorrente sono riusciti a disconnettere la postazione della segretaria e a prendere tutte le credenziali, anche l'OTP, inseriti dalla stessa per effettuare il bonifico voluto; successivamente quei dati sono stati inseriti entro un tempo molto ristretto, incluso lo stesso OTP, mentre gli SMS inviati presumibilmente dal resistente, senza che siano stati però ricevuti dalla segretaria in qualità di referente operativa, comunque costituiscono un elemento irrilevante dal momento che si deve ritenere che la tecnica del "man in the browser" abbia consentito a terzi malintenzionati di operare direttamente dalla postazione della vittima. Tutto considerato, la parte istante conclude chiedendo all'ABF quanto segue:

Accertare e dichiarare [redacted] responsabile per i motivi esposti in narrativa della frode avvenuta nei confronti della [redacted] e condannare la stessa al rimborso dell'intera somma illegalmente sottratta pari a €.42.500,53 secondo quanto prescritto dalla normativa sui servizi di pagamento e dalle disposizioni di cui al Codice della Privacy ed in particolare degli artt. 24, 32, 82 del GDPR. Con vittoria delle spese di lite, onorari e competenze, come da fattura allegata.

Convenuto ritualmente, l'intermediario eccepisce che la società ricorrente è titolare del conto corrente n. **20, acceso presso la filiale di XX del resistente, al quale è collegato il servizio di Home Banking Business che consente alle imprese di gestire on line i rapporti bancari. L'operazione di cui si chiede il rimborso risale ad un periodo precedente alla entrata in vigore, in Italia, della nuova normativa europea, nota come PSD2, avvenuta con decorrenza 14.09.2019. Tuttavia, il sistema di internet banking, anche prima della entrata in vigore della normativa europea PSD2, prevedeva già un sistema di autenticazione "forte" nella fase dispositiva, che includeva le credenziali di accesso (codice utente, codice postazione e password di accesso) e le credenziali di firma, tra cui una password dinamica e temporizzata (codice OTP) emessa da hardware Token (token fisico); in fase di primo accesso viene inviato al numero di cellulare del supervisore un SMS di benvenuto e, nel caso specifico, l'SMS è stato inviato al numero 339***933, il giorno 11.09.2018, come dimostrato dal dettaglio degli sms; solo in fase di secondo accesso, all'utente viene richiesto di autenticare la sua postazione di lavoro attraverso la digitazione di un codice OTP inviato dal resistente via SMS al cellulare del supervisore, al fine di certificare la postazione e, nel caso specifico, l'SMS contenente il codice OTP è stato inviato sempre al cellulare 339***933, il giorno 20.09.2018 come dimostrato dal dettaglio degli sms allegato al ricorso. Solo qualora il sistema di sicurezza del resistente rilevi una attività accomunabile ad un cambio di postazione di lavoro, viene richiesto all'utente di digitare un OTP inviato automaticamente dalla banca via SMS sul cellulare del supervisore ed è il supervisore a fornire il codice OTP, ricevuto via SMS sul proprio cellulare all'eventuale altro utente, che sta operando. Il 25.09.2018, il giorno dell'operazione contestata, il sistema ha inviato al cellulare richiamato un SMS contenente il codice OTP necessario per consentire l'accesso da una nuova postazione. Secondo le affermazioni dell'intermediario, alla sicurezza dell'home banking contribuisce anche il protocollo internet utilizzato, ossia un sistema HTTPS che garantisce sicurezza rafforzata e una comunicazione criptata; il tipo di operatività disconosciuta dalla ricorrente si rende possibile solo nel caso in cui il presunto frodatore sia a conoscenza delle credenziali di sicurezza dell'home banking, che può avere carpito esclusivamente al cliente.

Nel caso di specie, parte ricorrente non ha denunciato lo smarrimento o il furto o la perdita di possesso dei propri strumenti di sicurezza. Il ricorrente, invece, insiste sulla circostanza che si tratti di un caso di man in the browser, ma afferma altresì che i propri tecnici avevano rilevato la presenza di un malware, il Trojan Downloader.XXX, scaricato il giorno prima dell'operazione contestata, come allegato di un messaggio posta elettronica. Dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi, le operazioni risultano correttamente autenticate, registrate e contabilizzate; l'operazione essendo stata disposta come bonifico urgente, non avrebbe potuto in alcun modo essere bloccata. In ogni caso, la parte resistente è intervenuta presso la banca corrispondente per effettuare il richiamo dei fondi ma l'azione non ha avuto esito positivo. Per quanto attiene al trattamento dei dati personali, opera nel rispetto della normativa di riferimento, come da "Informativa sul trattamento dei dati personali" resa contestualmente alla sottoscrizione del contratto di apertura di conto corrente intestato alla società ricorrente; la questione sollevata dalla ricorrente non ha alcuna rilevanza nella valutazione della fattispecie sottoposta all'esame di codesto Collegio e non può neppure essere oggetto di esame da parte di codesto Collegio a causa della carenza di competenza in materia, riservata in via esclusiva al cd. Garante della Privacy.

Eccependo anche che nessuna assistenza di tipo professionale è espressamente richiesta ai fini della presentazione di un ricorso ABF, l'intermediario chiede all'Arbitro di respingere il ricorso in ogni sua parte perché infondato nel merito.

Parte ricorrente replica alle controdeduzioni del resistente, asserendo che la segretaria è chiaramente la persona identificata dal sottoscrittore come colei che riceve e utilizza gli strumenti di sicurezza dei servizi (Numero Cliente e PIN, fisso e senza alcun cambio imposto), dunque la stessa poteva accedere al conto corrente in oggetto tramite il sistema di internet banking, ed è questo che lei ha effettuato nel brevissimo periodo di utilizzo del servizio, in quanto la frode è occorsa dopo soli 15 giorni dalla consegna delle credenziali da parte dell'intermediario; ogni operazione dispositiva era sempre validata dal sottoscrittore e segnatamente dal titolare tramite l'inserimento dell'OTP temporizzato fornito tramite l'hardware token; con specifico riguardo al modulo "scheda informativa del cliente", questo riportava il solo numero di cellulare comunicato al resistente e si trattava specificatamente di quello della segretaria, ossia il numero 339***933; tuttavia, la segretaria non aveva accesso al Token Hardware e pertanto non poteva inserire direttamente gli OTP, poiché all'epoca dei fatti il token era custodito in cassaforte sotto la supervisione esclusiva del titolare; la procedura interna prevedeva, infatti, che la segretaria predisponesse sul piano amministrativo le operazioni, ma solo il titolare poteva decidere in via esclusiva di validarle e di approvarle effettuando le operazioni dispositive. Qualora il trojan horse fosse stato identificato in via automatica è probabile che la frode non si sarebbe verificata, visto che la tipologia di trojan horse rilevata è strettamente connessa alla frode del tipo man in the browser. Secondo la parte istante, nessuna inadempienza può essere imputata alla società ricorrente, in quanto la frode subita è stata certamente complessa e molto insidiosa, operata tramite una pianificata azione - tra trojan horse, sito clone e malware - mirata nei confronti dei clienti dell'intermediario. Ribadendo lamentele sulle carenze del sistema del resistente, la parte istante ribadisce le richieste espresse con il ricorso.

In controreplica, l'intermediario nel confermare quanto dichiarato nelle controdeduzioni, il resistente precisa che non ci sono stati malfunzionamenti nelle procedure, in quanto l'operazione è stata correttamente autenticata, registrata e contabilizzata; per quanto concerne il tipo di frode, il resistente precisa che il presunto attacco è avvenuto a carico dei

sistemi informatici dell'azienda ricorrente, non dell'intermediario che ne è del tutto estraneo; invece, l'intermediario ha adottato tutte le misure necessarie di sicurezza per la tutela del cliente, tra cui la firma digitale remota che si esercita con l'inserimento di un codice PIN e un codice OTP dinamico, fornito di volta in volta dallo strumento Hardware Token; secondo l'intermediario, l'esecuzione del bonifico contestato è avvenuta a causa della negligenza della ricorrente che ha continuato ad operare nonostante l'intercettazione sul PC dello stesso antivirus; la parte istante non ha denunciato lo smarrimento o il furto dei propri strumenti di sicurezza, denotando quindi una colpa grave nella loro custodia. Anche l'intermediario ribadisce le posizioni conclusive espresse nelle controdeduzioni.

DIRITTO

Parte ricorrente disconosce un'unica operazione di bonifico, dell'importo di € 42.500,53, eseguita in data 25.09.2018 tramite Home Banking e addebitata sul conto corrente intestato alla società. In relazione alle circostanze oggetto dell'odierna controversia, la società ricorrente ha sporto denuncia alle autorità competenti per "frode informatica", ricostruendo la vicenda negli stessi termini di cui all'odierno ricorso. In virtù della data di esecuzione dell'operazione contestata, ossia 25.09.2018, al caso di specie non risultano applicabili ratione temporis gli artt. 1, lettera qbis e l'art. 12, comma 2-bis del D.Lgs. n. 11/2010, concernenti la c.d. autenticazione forte (SCA). Nondimeno, già precedentemente all'entrata in vigore della normativa di attuazione della c.d. PSD2, i Collegi rilevano (si vedano, ex multis: Collegio di Torino, decisione n. 15639/2018, Collegio di Roma, decisione n. 14925/2017, Collegio di Bologna, decisione n. 7666/2017, decisione n. 1501/2022) la necessità di un sistema di autenticazione multifattoriale, in linea con le raccomandazioni delle medesime autorità di settore (tra cui la stessa EBA). Dunque, nonostante l'operazione disconosciuta risalga ad un periodo precedente alla entrata in vigore, in Italia, della normativa europea PSD2, avvenuta con decorrenza 14.09.2019, nelle controdeduzioni l'intermediario chiarisce che le modalità di accesso previste all'epoca dell'operazione prevedevano comunque una autenticazione forte nella fase dispositiva, attraverso codici che sono noti solo al cliente, di cui: uno statico, il PIN/Password; l'altro dinamico e temporizzato emesso di volta in volta, ossia l'OTP. L'intermediario eccepisce che l'operazione di bonifico contestata è stata regolarmente autenticata, registrata e contabilizzata ed è stata perfezionata mediante l'inserimento delle credenziali di accesso e delle credenziali di firma, ossia mediante una password dinamica e temporizzata (codice OTP) emessa da hardware token (token fisico). A sostegno delle proprie eccezioni, produce documentazione, corredata da apposita legenda esplicativa, che il Collegio riscontra. Da tale evidenza si evince che, come precisato dallo stesso resistente, il giorno dell'operazione contestata l'intermediario ha inviato all'utenza numero 339***933, SMS contenente il codice OTP necessario per "Attivare il nuovo dispositivo"; il numero di telefono richiamato è nell'esclusiva titolarità della segretaria della società ricorrente, la quale è referente operativa della società, come comprovato dal modulo di adesione al "Servizio Assistenza Imprese".

Con le controdeduzioni sono allegati i documenti tecnici e log da cui si desume l'autorizzazione dell'operazione dispositiva in oggetto e di cui l'intermediario fornisce spiegazione in narrativa.

Con riferimento al ricorso in oggetto, questo Collegio verifica che non sono riscontrati indicatori di anomalia di cui all'art. 8 (Rischio di frode) del D.M. 30.04.2007, n. 112 (Regolamento di attuazione della l. n. 166/2005, sulla "Istituzione di un sistema di prevenzione delle frodi di pagamento").

Parte ricorrente lamenta la "mancanza di un canale out-of-band, atteso che il cliente non viene informato sulle singole operazioni dispositive, né degli accessi effettuati sul sistema di internet banking". Dall'altro lato, l'intermediario, in proposito, precisa che la ricorrente "il 25.09.2018, prima dell'operazione dispositiva di cui si chiede il rimborso, ha ricevuto un sms contenente il codice OTP necessario per operare da nuova postazione, a fronte del quale non ha assunto iniziative". Dalla documentazione contrattuale versata in atti non emergono riferimenti ai sistemi di alert.

In punto di colpa, il Collegio di Coordinamento, n. 22745/19 ha fissato il seguente principio: "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". Dunque l'intermediario, (solo) dopo aver fornito prova della corretta autenticazione da parte dell'Intermediario, è chiamato 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".

Nel caso di specie l'intermediario, nelle proprie controdeduzioni, eccepisce che la società cliente non ha adempiuto agli obblighi di custodia degli strumenti di sicurezza, di cui non ha denunciato lo smarrimento o il furto, ragion per cui "è possibile che gli stessi le siano stati temporaneamente sottratti e, a sua insaputa, che qualcuno abbia avuto modo di inserire i dati necessari al completamento dell'operazione di bonifico".

Secondo quanto rappresentato dalle parti e sulla base della documentazione a disposizione, il Collegio ravvisa che la frode subita dalla ricorrente è stata generata da un malware, il "Trojan Downloader.XXX" identificato dal sistema antivirus del computer e scaricato il giorno prima della truffa come allegato di un messaggio di posta elettronica. In proposito, l'intermediario osserva che "già all'epoca dei fatti fosse noto ai più che si dovesse diffidare da email e/o link sconosciuti e non verificati prima di accedervi; inoltre se il malware era stato identificato dal sistema antivirus, marca Kaspersky, installato sul medesimo PC si sarebbe dovuto procedere con la bonifica del pc prima di continuare ad utilizzarlo e soprattutto prima di effettuare nuovi accessi a home banking, operazione che evidentemente non è stata, negligentemente, effettuata".

In punto di diritto, assumono particolare rilevanza le decisioni n. 3498/2012 e 1820/2013 del Collegio di Coordinamento ABF, con le quali sono state distinte le truffe realizzate mediante metodi ormai conosciuti alla clientela (le classiche e-mail di phishing), dalle truffe più insidiose in cui maggiore è la difficoltà di avvedersi della situazione di apparenza generata dal malware. In particolare, il Collegio di Coordinamento ha distinto:

a) le ipotesi di phishing tradizionale caratterizzate dall'invio di un semplice messaggio telefonico (cd. vishing), e-mail (cd. smishing) o SMS (cd. smishing) con il quale si invita il

cliente a digitare le proprie credenziali di accesso; molti dei tentativi di truffa posti in essere in materia di servizi di pagamento si svolgono secondo tale schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, SMS o altri strumenti di comunicazione, a comunicare e/o adinserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza;

b) la forma, più insidiosa, consistente in un "subdolo meccanismo di aggressione [che]ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino".

Tra le due fattispecie vi è una differenza tale da indurre a ritenere che solamente nella seconda, consistente in una sofisticata intrusione nell'autentico sito dell'intermediario nel momento in cui l'utente vi accede per compiere un'operazione, debba escludersi la sussistenza di una colpa grave del cliente. Con questa truffa sofisticata ed insidiosa del meccanismo frodatorio del Man in the Browser(MITB), i Collegi ABF ritengono che la condotta della parte vittima di attacco non sia connotabile da colpa grave.

Nel caso di specie, questo Collegio dà rilievo al fatto che è condiviso dalle parti, nonché attestato da analisi tecnica svolta nei giorni immediatamente successivi alla truffa, che il ricorrente avesse installato il Sistema Operativo Windows 10 ed avesse allestito il sistema di protezione antivirus marca Kaspersky "le cui definizioni venivano costantemente aggiornate tramite internet". Il tecnico di parte ricorrente conferma la presenza del malware, il "Trojan XXX" e, nella stessa data immediatamente successiva alla truffa, procede alla sua eliminazione.

Orbene, sulla presenza di Man in the Browser(MITB), i Collegi ABF, in linea con quanto già statuito dalle succitate decisioni del Collegio di coordinamento, convengono che la condotta del ricorrente vittima di tale attacco non sia connotata da colpa grave, salva la sussistenza di ulteriori elementi (quali, a titolo esemplificativo, la sua inerzia nel caso abbia rilevato anomalie del computer). Ma nel caso di specie, al contrario, il ricorrente ha dato prova di aver preservato il computer aziendale con il sistema di protezione antivirus, facendo ritenere scusabile, per questo Collegio, la sua negligenza nel non aver compreso gli eventuali messaggi di alert pervenuti dal software antivirus, messaggi di cui peraltro non si ha prova siano stati effettivamente prodotti dal software stesso.

Il Collegio conclude, in linea con la sua costante giurisprudenza (ex multis, Collegio Bologna decisione n. 2772/2020, n. 20430/2021), escludendo l'imputabilità al ricorrente del profilo di colpa grave, dovendo risultare il cliente indenne dalle perdite subite. Non accolto invece è il rimborso delle spese legali, che, secondo le più recenti posizioni condivise dai Collegi (ex multis, Collegio di Bologna, decisione n. 18966 del 23.8.2021) e in linea con l'orientamento già espresso nella pronuncia del Collegio di coordinamento n. 3498/2012, è ammesso solo quando l'ausilio di un legale si sia rivelato necessario per la complessità della controversia, circostanza che non si ravvisa nel caso di specie.
Tutto considerato, per questo Collegio il ricorso viene accolto parzialmente accertando il diritto della parte istante alla ricezione delle risorse finanziarie sottratte con la truffa subita, per un importo complessivo di 42.501 euro; trattandosi di ricorso presentato successivamente all'entrata in vigore delle nuove Disposizioni ABF, ai sensi di quanto

previsto nella nota (3) di pag. 25 delle predette Disposizioni, l'importo finale è arrotondato all'unità di euro, per eccesso stante la prima cifra dopo la virgola, dell'importo domandato (i.e. € 42.500,53), superiore a 5.

P.Q. M.

Il Collegio in parziale accoglimento del ricorso dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 42.501,00 (..omissis…).