DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Frodi nelle operazioni di pagamento e profili di responsabilità

Orientamenti ABF ed evoluzione normativa

Maggio 2024

Fabio Civale, Civale Associati

Fabio Civale, Civale Associati

Fabio Civale

Fabio Civale, avvocato. La sua attività, professionale e scientifica, è dedicata alle tematiche del diritto bancario e del diritto dei mercati finanziari. Collabora abitualmente con riviste giuridiche e giornali economici. È docente in master post laurea e convegni di interesse nazionale ed internazionale. È autore di libri e di numerose pubblicazioni in tema di diritto bancario e diritto dei mercati finanziari.

Sommario: 1. Tecniche di frode e *social engineering*. 2. Rimborso "immediato" (ma solo) per le operazioni non autorizzate. 3. Obblighi delle parti in relazione all'emissione e utilizzo di strumenti di pagamento. 4. Responsabilità per le operazioni oggetto di frode. 5. Onere della prova e di allegazione. 6. La colpa grave dell'utente per le operazioni oggetto di frode. 7. Aspettando PSD 3 ed il nuovo Regolamento PSR.

1. Tecniche di frode e social engineering

Sebbene recenti evidenze ([1]) mostrino come i requisiti di autenticazione forte (c.d. *Strong Customer Authentication*) ([2]) imposti dalla Direttiva PSD 2 ([3]) siano stati in grado di ridurre il rischio di frode per i pagamenti eseguiti da remoto, l'impatto (quantomeno percepito) delle frodi connesse agli strumenti di pagamento è cresciuto negli ultimi tempi ([4]).

1) *Cfr.* Banca d'Italia, *The security of retail payment instruments: evidence from supervisory data*, in *Markets, Infrastructures, Payment Systems*, January 2023; EBA, *Draft EBA Opinion on new types of payment fraud and possible mitigants*, April 2024 (EBA-Op/2024/01).

2) *Cfr.* art. 1, comma 1, lett. q-*bis* del D.lgs. n. 11/2010, laddove per "*autenticazione forte del cliente*" si intende "*un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*".

3) *Cfr.* Direttiva 2015/2366/UE del 25 novembre 2015 (c.d. PSD 2).

4) Il tema della responsabilità per le operazioni di pagamento oggetto di frode è stato ampiamente affrontato in dottrina. Sul punto si veda Semeraro, *Modelli di responsabilità e private enforcement: appunti su PSD2 e operazioni di pagamento non autorizzate*, in *Riv. Dir. Banc.* 2022, 825; Muttini, *Frodi informatiche e responsabilità della banca: i nuovi orientamenti dell'arbitro bancario finanziario*, in *Riv. Dir. Banc.*, 2021, 41; Cirelli, *Utilizzo non autorizzato dello strumento di pagamento e responsabilità della banca*, in *Giur. Comm.*, 2022, 438 ss.; Frau, *Home banking, phishing e responsabilità civile della banca, in Resp. civ. prev.*, 2019, 622 ss.; De Stasio, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, Paglietti - Evangelisti, *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, Roma, 2020; Berti De Marinis, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva "PSD2"*, in *Dir. banc. fin.*, 2018, 627; Malvagna, *Clausola di riaddebito e servizio di pagamento. Una ricerca sul rischio d'impresa*, 2018, Milano; Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione della responsabilità. Dagli orientamenti attuali alla revisione della PSD*, in *Dir. banc. fin.*, 2017, 150 ss; Martinelli, *Sicurezza informatica degli istituti di credito e responsabilità contrattuale*, in Giur. it., 2017, 2069 ss.; Marasà, *Utilizzo fraudolento di carta bancomat e diligenza professionale della banca*, in BBTC., 2016, 396 ss.; Maffeis, *Ordini di pagamento e di investimento "on line" nella giurisprudenza di merito e nella fonte persuasiva dinamica dell'Abf*, in Riv. dir. civ., 2013, 1273.

vedi l'articolo online

Alle tecniche di frode "tradizionali" si sono dapprima affiancate e poi sostituite le tecniche di c.d. *social engineering* che costituiscono il mezzo utilizzato da parte di frodatori per disporre, o più frequentemente far disporre allo stesso utente, operazioni di pagamento che vedono come beneficiari (finali) gli stessi frodatori.

I casi più diffusi e frequenti di frodi sono oggi classificati quali:

- ***phishing***, ossia l'invio di una e.mail o il rinvio ad un sito web "civetta" che simulano i canali istituzionali del prestatore di servizi di pagamento, ma che in realtà sono stati inviati o costruiti con l'unico scopo di raggirare gli utenti e carpire loro le credenziali di sicurezza personalizzate;

- ***whaling***, ossia una variante del *phishing*, basata su richieste di aggiornamento software in particolare rivolte a dirigenti e dipendenti di aziende ed imprese;

- ***maleware***, ***virus*** e ***keylogger***, ***man in the browser*** [5] ossia software dannosi in grado di registrare la digitazione di password e codici di accesso;

- ***qrishing***, ossia QR Code manipolati che reindirizzano a siti web fraudolenti;

- ***smishing***, tecnica simile al *phishing*, che si avvale di messaggi di testo per indurre in errore i clienti, invitandoli ad aprire *link* dannosi con lo scopo di sottrare loro i dati personali o indurli a comunicare le proprie credenziali/informazioni personali;

- ***vishing*** o ***voice phishing***, ossia la truffa telefonica con cui il frodatore cerca di indurre la vittima a fornire dati personali, fingendosi un dipendente / incaricato della banca o del prestatore di servizi di pagamento. Per concretizzare tale tecnica, il terzo frodatore utilizza tecniche di persuasione, di inganno ed in grado di ledere la capacità cognitiva e di giudizio della vittima;

- ***spoofing*** che rappresenta una tecnica complementare a quelle sopra indicate che consiste nel falsificare l'origine della connessione (indirizzo mittente della mail / numero di telefono) in modo da far credere che il contatto provenga dal prestatore di servizi di pagamento;

- ***ID caller spoofing*** ossia una telefonata nel corso della quale un sedicente operatore del prestatore di servizi di pagamento induce la vittima nella falsa rappresentazione di dover fornire dati e credenziali al fine di bloccare un'operatività fraudolenta, ovvero di stornare operazioni non autorizzate.

In aggiunta al rilievo penale di tali fattispecie che possono configurare casi di furto di identità digitale, le predette tecniche evolute di frodi hanno posto nuovamente il tema sicurezza ed efficienza degli strumenti di pagamento al centro dell'attenzione del legislatore europeo nel progetto di revisione della PSD ed occupa, in modo rilevante, i prestatori di servizi di pagamento chiamati ad approntare idonei presidi

5) Sul punto, il Collegio di Coordinamento dell'ABF, con la Decisione n. 3498 del 26 ottobre 2012, ha delineato i tratti tipici e l'operatività della fattispecie del *man in the browser*, così riassumendoli: "*Il principio operativo di tale meccanismo di intrusione viene definito in gergo man- in-the-browser a significare l'interposizione che questo genere di malware è in grado di operare fra il sistema centrale dell'intermediario e quello del singolo utente. Nella sua massima espressione di efficienza aggressiva, il programma malevolo, una volta annidatosi in un certo numero di computer, genera quella che in gergo suole definirsi una botnet, ossia per l'appunto una rete di macchine egualmente infettate dallo stesso virus. Il malware – riconducibile alla più ampia categoria dei cc.dd. trojan ("cavalli di Troia") e dotato di sofisticate capacità di elusione dei migliori antivirus – si annida in modo silenzioso nel computer della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il malware resta completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino (targeted banks). In quel preciso istante il malware "si risveglia" ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario. L'unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente, è la stringa di descrizione della pagina che, a differenza di quella originale, reca un prefisso di accesso (c.d. protocollo di trasferimento ipertestuale, Hyper Text Transfer Protocol) "http" e non già "https" (dove la "s" finale sta per secured, protetto). Ignaro dell'intervenuta sostituzione della pagina, l'utente è indotto a ritenere di trovarsi nel normale ambiente sicuro in cui normalmente egli opera. A quel punto il malware attiva una finestra a modulo, che pare sempre provenire dal sito dell'intermediario in cui si trova (crede di trovarsi l'utente, ove è richiesta una conferma di sicurezza con l'invito a compilare i campi del modulo con i propri dati e il codice generato dal dispositivo OTP: procedura che gli intermediari stessi talora attivano per controlli di sicurezza (specie come quando, nel caso in esame, l'accesso abbia luogo da una macchina diversa da quella abitualmente utilizzata dall'utente e come tale segnalata al server della banca da un differente indirizzo di provenienza: c.d. IP, Internet Protocol), il che rafforza nell'utente il convincimento della piena regolarità della situazione e della normalità del controllo automaticamente disposto dal sistema. L'utente, con ciò doppiamente ingannato, compila quindi i campi del modulo che il malware Pag. 13/19 prontamente trasmette all'intruso. Questi, così callidamente interpostosi nell'operazione, ha modo di captare tutti i fattori di autenticazione e di utilizzarli in tempo reale, nel mentre l'utente viene ulteriormente ingannato da un messaggio di attesa che, qualche minuto dopo, si conclude con la segnalazione dell'impossibilità di procedere all'operazione e con l'invito a ritentare in un secondo momento.*"

per la dovuta sensibilizzazione ed informazione della clientela, nonché per la prevenzione e mitigazione dei rischi di frode.

In tale contesto i profili di responsabilità per le operazioni di pagamento oggetto di frode meritano di essere analizzati, tanto alla luce delle letture più recenti fornite dall'ABF ([6]), quanto in relazione all'avviato progetto di revisione della disciplina europea dei servizi di pagamento ([7]).

6) Nella Relazione annuale pubblicata sul sito internet dell'Arbitro Bancario Finanziario in data 6 luglio 2023, in merito ai ricorsi su utilizzi fraudolenti di servizi e strumenti di pagamento, si legge che "*La digitalizzazione dei servizi e degli strumenti di pagamento sta modificando la dimensione, la forma, la frequenza e l'impatto degli utilizzi fraudolenti: secondo uno studio condotto a livello globale, tra il 2019 e il 2021 gli attacchi fraudolenti online hanno registrato un tasso di crescita molto più alto di quello delle transazioni online concluse regolarmente (rispettivamente 233 e 65 per cento). Le più recenti statistiche pubblicate dalla Banca d'Italia confermano la crescente diffusione in Italia dei servizi e degli strumenti di pagamento digitali tra il pubblico, sia in termini di unità sia di valore delle transazioni. Come in altri paesi, l'uso del contante si è ulteriormente ridotto durante la crisi pandemica. Questo andamento si è riflesso sulla composizione del contenzioso sottoposto all'ABF: nel periodo 2017-2022 il numero dei ricorsi inerenti agli utilizzi fraudolenti di strumenti di pagamento è aumentato di oltre 130 punti percentuali*".

7) La Commissione Europea ha pubblicato il 28 giugno 2023 un pacchetto legislativo, contenente una proposta di Direttiva e due proposte di Regolamento, ossia:
- "*Proposal for a Directive on payment services and electronic money services in the internal market (PSD3)*";
- "*Proposal for a Regulation on payment services in the internal market (PSR)*";
- "*Proposal for a Regulation on a framework for financial data access*".

La Proposta di Direttiva sui servizi di pagamento, che supererà l'attuale Direttiva PSD 2 costituirà la PSD 3, contiene misure finalizzate a mitigare le frodi nei pagamenti, migliorare i diritti dei consumatori, migliorare il funzionamento e l'efficienza dell'*open banking*, introdurre condizioni di parità tra le banche e i fornitori di servizi di pagamento diversi dalle banche al fine di ridurre i costi.
La Proposta di Regolamento sui servizi di pagamento (PSR) ha l'obiettivo di recepire le norme stabilite all'interno della proposta di Direttiva PSD3 rendendole direttamente applicabili.
Infine, la Proposta di Regolamento su un quadro normativo per l'accesso ai dati finanziari stabilisce diritti e obblighi finalizzati a gestire la condivisione dei dati dei clienti nel settore finanziario, con l'obiettivo di sviluppare prodotti e servizi finanziari più innovativi e stimolare la concorrenza nel settore finanziario. Tra le misure proposte si segnalano la possibilità per i clienti, ma non l'obbligo, di condividere i propri dati con i "*data users*" (soggetti che hanno il diritto di accedere ai dati forniti dai clienti), l'obbligo di mettere tali dati a disposizione dei "data users" da parte dei "*data holders*" (soggetti che raccolgono ed elaborano i dati), fermo il pieno controllo da parte dei clienti dei propri dati.
In data 24 aprile 2024 il Parlamento Europeo ha approvato in prima lettura, con emendamenti, la proposta relativa alla PSD 3 ed al Regolamento PSR.

2. Rimborso "immediato" (ma solo) per le operazioni non autorizzate

Un primo tema attiene ai presupposti del diritto dell'utente ad ottenere il rimborso "immediato" per le operazioni non autorizzate.

Come noto, l'art. 11 del d. lgs. 11/2010 prevede che in caso di operazioni di pagamento "*non autorizzate*" il pagatore abbia diritto al rimborso entro la fine della giornata operativa successiva a quella in cui il prestatore di servizi di pagamento prende atto dell'operazione eseguita in assenza di autorizzazione.

Tale rimborso, di fatto immediato, può essere sospeso solo in caso di "*motivato sospetto di frode*" riconducibile all'utente ([8]) ed a condizione che sia data comunicazione all'Autorità di Vigilanza da parte del prestatore di servizi di pagamento. Il rimborso non preclude la possibilità per il prestatore di servizi di pagamento di dimostrare, anche in un momento successivo, che l'operazione era stata autorizzata e di ri-addebitare il conto dell'utente.

Il presupposto che fonda il diritto dell'utente ad ottenere il rimborso entro la fine della prima giornata operativa successiva al *claim* è chiaramente indicato dalla norma italiana e comunitaria ([9]) ed è rappresentato dalla sussistenza di una "*operazione di pagamento non autorizzata*".

Anche per quanto si dirà in seguito, risulta essenziale considerare che una operazione di pagamento può considerarsi non autorizzata qualora sia carente il consenso del pagatore, prestato nella forma e secondo la procedura concordata nel contratto quadro PSD.

Qualora l'operazione sia priva del consenso dell'utente la stessa operazione non è autorizzata e, quindi, si impone un rimborso subitaneo. Diversamente, qualora sussista il consenso dell'utente, ossia in caso di operazione autorizzata, non si integra il presupposto per l'applicazione del rimborso "immediato" secondo quanto previsto dall'art. 11 del d. lgs. 11/2010.

Nell'ambito di tale "ritmo binario" (operazione autorizzata – operazione non autorizzata), su cui si basa

8) Si veda il considerando n. 71 della Direttiva PSD 2.
9) L'art. 11 del D.lgs. 11/2010 è frutto del recepimento dell'art. 73 della Direttiva PSD 2.

vedi l'articolo online

l'attuale e vigente disciplina europea e nazionale, occorre incasellare anche i casi controversi di operazioni in cui il consenso dell'utente sussiste, risulta essere stato prestato nella forma e secondo la procedura concordata nel contratto quadro PSD, ma l'utente afferma essere stato carpito con artifizi e raggiri posti in essere da terzi frodatori. Per tali operazioni oggetto di frode si è posta quindi la questione, evidentemente non puramente dogmatica, circa l'applicabilità o meno dell'art. 11 del d. lgs. 11/2010, questione che si risolve nello stabilire se le operazioni in cui il consenso dell'utente sussiste ma si affermi essere stato carpito con frodi di terzi siano o meno operazioni autorizzate.

Anticipando le conclusioni riferite a tale questione, si ritiene che, quantomeno stante al vigente quadro normativo, siano da ritenersi operazioni "autorizzate" (anche) le operazioni eseguite sulla base del consenso dell'utente, prestato nella forma e secondo la procedura concordata nel contratto quadro PSD, ma che si affermi essere stato oggetto di frode e che, quindi, non risulti applicabile per tali operazioni il diritto dell'utente ad ottenere il rimborso immediato ai sensi dell'art. 11 del d. lgs. 11/2010, fermo in ogni caso il diritto dello stesso utente ad invocare la responsabilità del prestatore di servizi di pagamento ai sensi dell'art. 12 del d. lgs. 11/2010.

Nel breve volgere del tempo indicato nell'art. 11 del d.lgs. 11/2010, ossia una giornata operativa, il prestatore di servizi di pagamento deve (e può) verificare (unicamente) l'esistenza o meno dell'autorizzazione dell'utente, rilasciata nella forma e secondo la procedura concordata nel contratto quadro PSD.

Nel termine di una giornata operativa il prestatore di servizi di pagamento non deve (né può) appurare se l'autorizzazione dell'utente sia "totalmente genuina" o sia frutto di una frode perpetrata da un terzo e che abbia visto come vittima lo stesso utente. Trattasi di accertamento complesso che richiede tempistiche più dilatate. Detto accertamento, oltre che di fatto precluso dalla stringente tempistica prevista dall'art. 11 del d. lgs. 11/2010, non risulta neppure richiesto dalla precitata norma che impone unicamente di accertare se sussista o meno una autorizzazione dell'utente, rilasciata nella forma e secondo la procedura concordata nel contratto quadro PSD.

Sarebbe al pari non esigibile in concreto e del resto non coerente con l'impianto normativo attuale esigere che il prestatore di servizi di pagamento, al fine di non procedere al rimborso, debba addurre l'esistenza del dolo e della colpa grave dell'utente ai sensi dell'art. 12 del d. lgs. 11/2010, predicandosi in modo non condivisibile una lettura congiunta degli articoli 11 e 12 del d. lgs. 11/2010, che restano

fattispecie distinte e che (non a caso) insistono in norme distinte.

Mentre il "*motivato sospetto di frode*" dell'utente di cui all'art. 11 del d. lgs. 11/2010 attiene alla sospensione del diritto di rimborso subitaneo e si configura in un comportamento frodatorio riconducibile all'utente, le fattispecie di "*dolo*" o "*colpa grave*" di cui all'art. 12 del d. lgs. 11/2010 attengono all'esclusione della responsabilità del prestatore di servizi di pagamento per le operazioni conseguenti ad un utilizzo non autorizzato di strumenti o servizi di pagamento. In caso di "*dolo*" o "*colpa grave*" dell'utente ai sensi dell'art. 12 del d. lgs. 11/2010 il rimborso non deve essere semplicemente sospeso, ma non è dovuto ai sensi dello stesso art. 12 del d. lgs. 11/2010.

In merito alla lettura dei presupposti di cui all'art. 11 del d. lgs. 11/2010 si è espressa Banca d'Italia con comunicazione del 30 ottobre 2023 avente ad oggetto "*Obbligo di segnalazione di cui all'art. 11 del D.lgs. 11/2010. Template per le comunicazioni alla Banca d'Italia*". Con tale Comunicazione Banca d'Italia ha inteso ricordare che i prestatori di servizi di pagamento possono sospendere il rimborso subitaneo dell'operazione non autorizzata nel caso in cui ravvedano un motivato sospetto di frode dell'utente. Banca d'Italia ha chiarito che il comportamento fraudolento si caratterizza per elementi specifici che denotano l'intenzione dell'utente (e non di un qualsiasi soggetto terzo) di raggirare il prestatore di servizi di pagamento e che tale comportamento intenzionale dell'utente non può consistere nella mera inosservanza dolosa o colposa degli obblighi di comunicazione e custodia sul medesimo gravanti *ex* art. 7 del d. lgs. 11/2010. La stessa Autorità di Vigilanza ha poi concluso che qualora il prestatore di servizi di pagamento disponga "*di elementi idonei a provare il comportamento fraudolento, doloso o gravemente colposo dell'utente e, quindi, a soddisfare l'onere probatorio di cui all'art. 10, comma 2 del Decreto, si ritiene risultino insussistenti i presupposti normativamente previsti per la sospensione del rimborso e per la relativa segnalazione alla Banca d'Italia*".

Ne consegue che nelle ipotesi in cui l'utente dei servizi di pagamento avanzi contestazioni riferibili ad una o più operazioni, il prestatore di servizi di pagamento deve procedere, nel termine di una giornata operativa, a verificare l'esistenza o meno di una valida autorizzazione dell'utente stesso, rilasciata nella forma e secondo la procedura concordata nel contratto quadro PSD.

Occorre procedere al rimborso *ex* art. 11 del d. lgs. 11/2010 qualora non sussista tale autorizzazione, ovvero qualora il prestatore di servizi di pagamento non sia in grado di accertare e dimostrare che l'operazione di pagamento sia stata correttamente autorizzata ([10]).

In tali casi – ossia di operazione priva di autorizzazione o di carenza di prova dell'autorizzazione - il rimborso può essere sospeso *ex* art. 11, comma 2, del d. lgs. 11/2010 solo qualora sussista un motivato sospetto di frode riconducibile all'utente, dovendosi dare informativa a Banca d'Italia di detta sospensione del rimborso ([11]).

Nella diversa ipotesi in cui l'operazione sia stata autorizzata ed il prestatore di servizi di pagamento sia in grado di accertare e dimostrare che l'operazione di pagamento è stata correttamente autorizzata,

10) Tale interpretazione troverebbe conferma anche in talune decisioni dell'Arbitro Bancario Finanziario, in cui la sussistenza del dovere di rimborso in capo all'intermediario ai sensi dell'art. 11, primo comma, del d. lgs. n. 11/2010 è diretta conseguenza del mancato assolvimento dell'onere probatorio gravante sull'intermediario. Sul punto, si richiama la Decisione ABF del Collegio di Bologna, n. 7648 del 13 maggio 2022, in cui si legge che "*In assenza della produzione da parte dell'intermediario di documentazione idonea a dimostrare la corretta e regolare autenticazione delle operazioni contestate, non può dirsi assolto l'onere probatorio gravante sull'intermediario di provare che le operazioni siano state regolarmente autenticate, correttamente registrate e contabilizzate, ai sensi dell'art. 10 del d.lgs. n. 11/2010, con l'effetto che le stesse vengono considerate come non autorizzate dalla parte ricorrente e, pertanto, alla medesima non opponibili, con conseguente sussistenza del dovere di integrale rimborso in capo all'intermediario ai sensi dell'art. 11 co. 1 del d.lgs. n. 11/2010 («Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo»)*". In senso conforme, si richiama un'ulteriore Decisione ABF del Collegio di Bologna, n. 7643 del 13 maggio 2022, nella quale si legge che "*In base al quadro normativo sopra delineato, così come corredato dagli interventi dell'EBA, non può che confermarsi che spetta all'intermediario la prova dell'intervenuta autenticazione forte delle operazioni di pagamento. Pertanto in difetto di tale prova questo Collegio considera le operazioni sopra individuate come non autorizzate dalla parte ricorrente e, pertanto, alla medesima non opponibili, con conseguente sussistenza di un dovere di integrale rimborso in capo all'intermediario ai sensi e nelle forme dell'art. 11, comma 1, d.lgs. n. 11/2010.*".

11) Tale sospetto di frode deve risultare "motivato", per meglio dire legato a motivazioni oggettivamente riscontrabili e documentabili da parte del prestatore di servizi di pagamento, non apparendo legittime ipotesi di sospensione del rimborso fondate su meri apprezzamenti dell'intermediario. Inoltre, i motivi che giustificano la sospensione del rimborso devono risultare dal complesso delle evidenze del caso di specie, non essendo legittima una sospensione del rimborso giustificata dall'esigenza di ricercare o escludere ipotesi di frode. La valutazione del prestatore di servizi di pagamento in merito all'esistenza di un sospetto di frode, ancorata - come detto - a dati oggettivamente riscontrabili, deve essere immediata rispetto alla richiesta di rimborso del cliente. Tale valutazione, peraltro, non deve giungere alla certezza dell'esistenza di una frode, potendosi ritenere legittima una sospensione del rimborso motivata anche da un qualificato "sospetto" di frode, purché fondato su dati oggettivi e riscontrabili.

non troverà applicazione l'art. 11 del d. lgs. 11/2010 in tema di rimborso immediato, ciò anche qualora l'operazione risulti autorizzata ma l'utente affermi l'esistenza di una ipotesi di frode di terzi ([12]), fermi i diritti dell'utente di cui all'art. 12 del d. lgs. 11/2010.

3. Obblighi delle parti in relazione all'emissione e utilizzo di strumenti di pagamento

La "ricerca" delle responsabilità in relazione alle operazioni di pagamento oggetto di frode, stando al vigente quadro normativo, deve essere svolta muovendo dagli obblighi che ciascuna delle parti deve rispettare in relazione agli strumenti di pagamento ([13]).

Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo ([14]) di:

a) assicurare che le credenziali di sicurezza personalizzate ([15]) non siano accessibili a soggetti diversi dall'utente legittimato ad usare lo strumento medesimo;

b) astenersi dall'inviare strumenti di pagamento non richiesti, a meno che lo strumento di pagamento già consegnato all'utente debba essere sostituito;

c) assicurare che siano sempre disponibili strumenti adeguati (ad esempio siti internet, call center, ecc.) attraverso cui l'utente dei servizi di pagamento possa eseguire la comunicazione di smarrimento, furto, appropriazione indebita, uso non autorizzato, nonché la richiesta di riattivazione dello strumento di pagamento o l'emissione di uno nuovo ove l'intermediario non vi abbia già provveduto;

12) Sul punto si richiamano le seguenti decisioni ABF: Collegio di Milano, Decisione n. 2006 del 15 febbraio 2024; Collegio di Milano, Decisione n. 1963 del 14 febbraio 2024; Collegio di Palermo, Decisione n. 33 del 2 gennaio 2024.

13) Per "*strumento di pagamento*" si intende "*qualsiasi dispositivo personalizzato e/o insieme di procedure concordate tra l'utilizzatore e il prestatore di servizi di pagamento e di cui l'utilizzatore di servizi di pagamento si avvale per impartire un ordine di pagamento*" (*cfr.* art. 1, comma 1, lett. s) del d. lgs. 11/2010)

14) *Cfr.* art. 8, comma 1, del d.lgs. 11/2010.

15) *Cfr.* art. 1, comma 1, lett. q-*ter* del D.lgs. n. 11/2010, laddove per "*credenziali di sicurezza personalizzate*" si intendono le "*funzionalità personalizzate fornite a un utente di servizi di pagamento dal prestatore di servizi di pagamento a fini di autenticazione*".

vedi l'articolo online

d) impedire qualsiasi utilizzo dello strumento di pagamento successivo alla comunicazione dell'utente di avvenuto smarrimento, furto, appropriazione indebita, uso non autorizzato.

Il novero degli obblighi in capo al prestatore di servizi di pagamento che emette uno strumento di pagamento appare estremamente ampio e l'utilizzo ripetuto dell'espressione "*assicurare*" indica chiaramente che si tratta di obblighi da assolvere attraverso la predisposizione ed il costante affinamento di requisiti organizzativi e procedure interne (specie di carattere informatico) volte a garantire l'inviolabilità dei sistemi attraverso i quali sono processate le operazioni di pagamento tra intermediario e cliente.

In aggiunta a quanto precede, i prestatori di servizi di pagamento devono applicare l'autenticazione forte del cliente quando l'utente: a) accede al conto di pagamento *on line*; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione tramite canale a distanza che può comportare il rischio di frode ([16]).

Come si indicherà nel successivo paragrafo, la responsabilità dei prestatori di servizi di pagamento per l'utilizzo non autorizzato di strumenti o servizi di pagamento è diretta conseguenza della violazione di uno o più degli obblighi che precedono.

Con tratto del tutto caratteristico della disciplina dei servizi di pagamento, la PSD prevede "*obblighi*" in relazione agli strumenti di pagamento ed alle credenziali di sicurezza personalizzate non solo in capo all'intermediario che presta il servizio di pagamento, ma anche in capo all'utente che è tenuto a "cooperare" per assicurare la sicurezza ed efficienza nel settore dei pagamenti.

L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo ([17]) di:

a) utilizzare lo strumento stesso in conformità con i termini, esplicitati nel contratto quadro PSD, che ne regolano l'emissione e l'uso;

b) adottare, non appena riceve uno strumento di pagamento, tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate;

c) comunicare, senza indugio, secondo le modalità previste nel contratto quadro PSD, all'intermediario o al soggetto da questi indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento "*non appena ne viene a conoscenza*".

Sull'utente incombono, quindi, sia obblighi di diligente custodia ed utilizzo dello strumento di pagamento e delle relative credenziali di sicurezza personalizzate, sia obblighi di tempestiva comunicazione all'intermediario dei casi di smarrimento, furto, appropriazione indebita o uso non autorizzato.

4. Responsabilità per le operazioni oggetto di frode

Ritenere che solo l'intermediario possa o debba, in qualità di prestatore di servizi, rispondere della fase patologica di utilizzo non autorizzato di uno strumento di pagamento, in quanto ascrivibile al rischio di impresa, finirebbe per addossare all'intermediario rischi che di per sé esulano dai poteri di controllo dello stesso prestatore di servizi ed, al tempo stesso, potrebbe comportare il rischio di deresponsabilizzazione dell'utente, con potenziali ricadute in termini di incrementi dei costi dei servizi per tutti gli utenti.

Tale approdo non solo non appare coerente all'attuale impianto normativo, europeo e nazionale, che come detto prevede obblighi in capo ad entrambe le parti (prestatore di servizi di pagamento e utente), ma neppure risulta utile ove si abbia realmente a cuore l'efficienza e la sicurezza dei servizi di pagamento.

Pur muovendo dal noto criterio del rischio di impresa e dalla necessità di assicurare tutela all'utenza, anche nell'ottica di ulteriore sviluppo degli strumenti di pagamento, appare opportuno non trascurare del tutto la necessità di una "collaborazione attiva" dell'utente che risulta di fatto essere decisiva ai fini di prevenire, limitare e arrestare i casi di utilizzo indebito degli strumenti di pagamento.

Affermare l'utilità di un (circoscritto) ambito di responsabilità per l'utente assolve non tanto ad una funzione di compartecipazione al rischio economico relativo ad utilizzi non autorizzati degli strumenti di pagamento, che resta sostanzialmente a carico dei singoli prestatori di servizi di pagamento, quanto

16) *Cfr.* art. 10 *bis* del d. lgs. 11/2010
17) *Cfr.* art. 7 del d. lgs. 11/2010

piuttosto alla funzione di incentivare l'utenza a prestare la dovuta collaborazione, attivandosi sia per preservare la riservatezza delle credenziali di sicurezza personalizzate, sia per comunicare tempestivamente i casi di furto, smarrimento o sottrazione degli stessi strumenti.

Nell'attuale impianto normativo si possono individuare sostanzialmente tre livelli di responsabilità per le operazioni di pagamento oggetto di frode, inderogabili nel caso di cliente consumatore o micro-impresa ([18]).

Ad un primo livello si colloca una responsabilità "esclusiva" del prestatore di servizi di pagamento. In particolare, l'utente non sopporta alcuna perdita in relazione ad utilizzi non autorizzati di strumenti di pagamento che siano diretta conseguenza di violazioni degli obblighi, richiamati nel precedente paragrafo, in capo al prestatore di servizi di pagamento ai sensi degli artt. 8 e 10 *bis* del d. lgs. 11/2010. Dalla violazione degli obblighi in capo al prestatore di servizi di pagamento non può che discendere una responsabilità esclusiva dello stesso. Ad esempio, risulta evidente che se il prestatore di servizi di pagamento non esige una autenticazione forte dell'utente, ovvero non ha inibito l'utilizzo di strumenti di pagamento che sono stati oggetto di segnalazione di smarrimento o di utilizzo non autorizzato, le conseguenze economiche delle operazioni di pagamento non possono che ricadere sul prestatore di servizi di pagamento.

Ad un secondo livello si collocano i casi in cui, pur non essendo riscontrabile una violazione in capo al prestatore di servizi di pagamento ai sensi degli artt. 8 e 10 *bis* del d. lgs. 11/2010, lo stesso prestatore è chiamato a sopportare il "rischio economico" delle operazioni non autorizzate salvo un contributo dell'utente non superiore ad Euro 50. In questo livello intermedio si coglie appieno l'applicazione del criterio di allocazione della perdita secondo il principio del rischio di impresa e l'esigenza di assicurare tutela all'utenza dei servizi di pagamento.

Ad un terzo livello (di spettro ridotto) si collocano i casi di responsabilità "esclusiva" dell'utente che sopporta integralmente le conseguenze economiche delle operazioni non autorizzate allorquando è riscontrabile una violazione con dolo o colpa grave dello stesso utente degli obblighi di cui all'art. 7 del d. lgs. 11/2010.

5. Onere della prova e di allegazione

Attingendo alla rilevante casistica ABF, si coglie con immediatezza la rilevanza delle tematiche connesse ai profili afferenti all'onere della prova e di allegazione.

Qualora il cliente neghi di aver autorizzato un'operazione di pagamento o contesti l'irregolare esecuzione, il prestatore di servizi di pagamento deve provare che "*l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*", ai sensi dell'art. 10, comma 1, del d. lgs. 11/2010 ([19]).

Il prestatore di servizi di pagamento è chiamato a provare, oltre all'insussistenza di malfunzionamenti nei propri sistemi informatici, l'autenticazione dell'utente, ossia la procedura attraverso cui lo stesso prestatore di servizi di pagamento verifica l'identità di un utente o la validità dell'uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore ([20]).

18) E'consentita una deroga, totale o parziale, a tali criteri di allocazione del rischio di uso abusivo di uno strumento di pagamento nei rapporti con i clienti diversi dai consumatori e microimprese. Anche in tal caso, peraltro, si ritengono applicabili i limiti posti all'autonomia delle parti in tema di esonero di responsabilità *ex* art. 1229 c.c., nonché le ipotesi di concorso del fatto colposo del creditore *ex* art. 1227 c.c..

19) Il secondo comma dell'art. 10 del d.lgs. 11/2010 prevede che, sempre qualora il cliente neghi di aver autorizzato un'operazione di pagamento, il mero utilizzo di uno strumento di pagamento non è di per sé "*necessariamente sufficiente*" a dimostrare il valido consenso del cliente, né tantomeno che sussista una ipotesi di frode o di inadempimento, con dolo o colpa grave, degli obblighi in capo al cliente di diligente custodia ed utilizzo dello strumento di pagamento ex art. 7 del d.lgs. 11/2010. La previsione, anche stando al suo contenuto letterale, non sembra volta ad escludere qualsivoglia valore probatorio all'utilizzo di uno strumento di pagamento ai fini della riconducibilità dell'operazione al cliente, quanto piuttosto appare diretta ad escludere che lo stesso (mero) utilizzo possa assurgere a mezzo di prova (*rectius* presunzione) di per sé "*necessariamente sufficiente*". In sostanza, ai fini della riconducibilità dell'operazione di pagamento al cliente, l'intermediario dovrà dimostrare (in positivo) sia l'utilizzo dello strumento di pagamento da parte del cliente (di per sé non "*necessariamente sufficiente*" in termini di prova, ma comunque elemento necessario), sia il corretto funzionamento delle procedure di ricezione ed esecuzione dell'ordine di pagamento.

20) *Cfr.* art. 1, comma 1, lett. q del D.lgs. n. 11/2010.

In tema di prova di autenticazione dell'utente, si riscontrano numerose decisioni dell'Arbitro Bancario e Finanziario che hanno affermato i seguenti principi:

a. in caso di mancata "completa" prova di autenticazione forte (SCA), la responsabilità per le operazioni di pagamento contestate ricade interamente sul prestatore di servizi di pagamento. Trattasi infatti di prova ritenuta prodromica rispetto a ogni altro elemento rilevante ai fini dell'accertamento della responsabilità, che assume valore assorbente anche rispetto alla valutazione di eventuali profili di colpa grave dell'utente ([21]). I c.d. *log file* attraverso cui l'intermediario fornisce prova del processo di autenticazione devono essere completi, ossia coprire l'intero processo autorizzativo, nonché essere sufficientemente chiari e comprensibili per l'organo decidente, ciò anche avvalendosi di idonee leggende illustrative che consentano di verificare i singoli passaggi che in concreto hanno condotto a un certo risultato registrato dal sistema informatico come prova di autenticazione;

b. l'autenticazione forte deve essere provata anche con riguardo a tutte le fasi prodromiche all'effettuazione delle operazioni di pagamento disconosciute (*login* all'area personale dell'utente anche tramite APP, eventuale modifica della *password* di accesso e/o dell'utenza telefonica associata all'area personale, eventuale revoca dell'utenza del cliente, eventuale registrazione di una nuova utenza di accesso all'area personale, ecc.)([22]);

c. in caso di c.d. *digital wallet* l'autenticazione forte è richiesta sia nella fase di accesso al conto / *enrollment* dell'app / registrazione della carta sul *wallet*, sia nella fase di esecuzione delle singole operazioni. Nel caso di c.d. carte *tokenizzate* l'utilizzo di un *wallet* affidato a un terzo gestore per l'esecuzione di operazioni di pagamento non esime il prestatore di servizi di pagamento dall'onere di fornire prova dell'autenticazione forte delle operazioni compiute. La prova deve riguardare tanto la fase di c.d. *tokenizzazione* della carta nel *wallet*, quanto la fase esecutiva delle singole operazioni ([23]);

d. il prestatore di servizi di pagamento deve essere in grado di provare l'invio dei codici OTP tramite sms ovvero l'invio della notifica *push* al dispositivo mobile associato alla carta/conto dell'utente (dimostrandone anche il relativo contenuto), l'eventuale attivazione del c.d. riconoscimento biometrico, nonché evidenza di quale sia il *device* sul quale è stata installata l'applicazione dei servizi di internet banking ([24]);

e. il prestatore di servizi di pagamento deve essere in grado di provare le evidenze dell'inserimento dei singoli fattori di autenticazione SCA, ovvero specificare i motivi per cui – nei log informatici – non siano stati valorizzati gli specifici "*campi*" relativi alla autenticazione ([25]).

Se indubbiamente grava sul prestatore di servizi di pagamento l'onere della prova di autenticazione dell'utente, come riconosciuto dall'Arbitro Bancario e Finanziario in capo all'utente sono previsti oneri di allegazione. In particolare ad avviso dell'ABF può determinare il rigetto del ricorso ([26]) la mancata allegazione da parte dell'utente del messaggio civetta ovvero della telefonata pervenuta dal sedicente operatore del prestatore di servizi di pagamento, in quanto tale carenza non consente di verificare se il mittente risulti riconducibile al prestatore di servizi di pagamento e fosse quindi possibile un legittimo affidamento dell'utente circa la genuinità del messaggio / contatto telefonico.

In aggiunta alla (e dopo la) prova di autenticazione dell'utente, il prestatore dei servizi di pagamento

21) *Cfr.* Collegio di Milano, Decisione n. 1963 del 14 febbraio 2024; Collegio di Bologna, Decisione n. 1905 del 14 febbraio 2023; Collegio di Milano, Decisione n. 1634 del 8 febbraio 2024; Collegio di Milano, Decisione n. 1612 del 6 febbraio 2024; Collegio di Milano, Decisione n. 1598 del 6 febbraio 2024; ; Collegio di Milano, Decisione n. 1460 del 1 febbraio 2024; Collegio di Torino, Decisone n. 643 del 15 gennaio 2024; Collegio di Bologna, Decisione del 12 gennaio 2024, n. 577; Collegio di Milano, Decisione n. 158 del 4 gennaio 2024.

22) *Cfr.* Collegio di Coordinamento, Decisione n. 13398 del 18 ottobre 2022; Collegio di Milano, Decisione n. 1964 del 14 febbraio 2024.

23) *Cfr.* Collegio di Coordinamento, Decisione n. 21285 dell'11 ottobre 2021; Collegio di Milano, Decisione n. 1964 del 14 febbraio 2024; Collegio di Milano, Decisione n. 1606 del 6 febbraio 2024; Collegio di Torino, Decisione n. 1487 del 2 febbraio 2024; Collegio di Bari, Decisione n. 388 del 9 gennaio 2024; Collegio di Palermo, Decisione n. 11980 del 4 dicembre 2023.

24) *Cfr.* Collegio di Milano, Decisione n. 905 del 20 gennaio 2024; Collegio di Bari, Decisione n. 1556 del 6 febbraio 2024.

25) Collegio di Bologna, Decisione n. 12476 del 13 dicembre 2023.

26) *Cfr.* Collegio di Milano, Decisione n. 1447 del 1 febbraio 2024; Collegio di Milano, Decisione n. 1171 del 25 gennaio 2024; Collegio di Milano, Decisione n. 225 del 5 gennaio 2024.

ove intenda invocare una responsabilità esclusiva dell'utente deve altresì "*fornire la prova della frode, del dolo o della colpa grave dell'utente*" ([27]). Si tratta di un onere oggettivamente gravoso che, sovente, è assolto ì avvalendosi delle dichiarazioni rese dall'utente (in sede di reclamo o di denuncia), nonché valorizzando le specifiche e concrete modalità della frode posta in essere che poteva essere "riconosciuta" o "limitata" dall'utente con un contegno minimamente diligente.

6. La colpa grave dell'utente per le operazioni oggetto di frode

La c.d. colpa grave si qualifica quale condotta connotata da straordinaria e inescusabile imprudenza o negligenza in cui l'utente dei servizi di pagamento omette di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti.

La colpa grave deve riferirsi ad una violazione di uno o più degli obblighi in capo all'utente, ai sensi dell'art. 7 del d. lgs. 11/2010, di diligente custodia ed utilizzo dello strumento di pagamento, ovvero di tempestiva comunicazione all'intermediario dei casi di smarrimento, furto, appropriazione indebita o uso non autorizzato.

La valutazione circa la sussistenza di una colpa grave dell'utente, per sua natura, deve essere condotta con riferimento alla specifica realtà fattuale, alle caratteristiche di sicurezza dello strumento di pagamento utilizzato, all'esistenza di eventuali sistemi di allerting per il cliente (e.mail, s.m.s., ecc.), alle caratteristiche soggettive ed al comportamento tenuto dell'utente di servizi di pagamento, al grado di riconoscibilità delle ipotesi specifiche di frode e di indebito utilizzo, al tempo trascorso tra il momento in cui il cliente ha avuto contezza della sottrazione dello strumento di pagamento e la richiesta di blocco, ecc..

Si tratta, in sostanza, di declinare in concreto gli obblighi civilistici di diligenza e custodia in capo al cliente per individuare il limite estremo della loro violazione ascrivibile a "colpa grave" dell'utente. Tale violazione può avere ad oggetto sia l'omissione degli obblighi di diligente custodia dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento (PIN, password, token, codici alfanumerici), sia un utilizzo dello strumento non conforme ai termini esplicitati nel contratto relativi all'emissione ed all'uso, sia l'omessa comunicazione tempestiva dei casi di smarrimento, furto, appropriazione indebita o uso non autorizzato.

Evidenziata la pluralità e la rilevanza delle variabili, di carattere oggettivo fattuale e soggettivo comportamentale, si possono individuare le seguenti situazioni sintomatiche che possono, si ripete in funzione del caso concreto, condurre a ritenere in capo all'utente una violazione con colpa grave degli obblighi di cui all'art. 7 del d. lgs. 11/2010:

- l'aver disvelato le credenziali di sicurezza personalizzate ai terzi frodatori ([28]);

- l'assenza di attinenza del "contatto" avvenuto tramite SMS o telefonata con i contatti del prestatore di servizi di pagamento ([29]);

- la mancata dovuta attenzione agli allert del prestatore di servizi di pagamento ricevuti dall'utente a mezzo e-mail, notifica push e sms, ovvero alle notifiche relative all'avvenuta richiesta di autorizzazione per l'esecuzione delle operazioni fraudolente ([30]):

- la circostanza che l'operazione disconosciuta sia stata effettuata da un indirizzo IP identico a quello relativo ad altre operazioni, effettuate in epoca anteriore, che l'utente non ha disconosciuto ([31]);

- l'avvenuta ricezione da parte dell'utente di comunicazioni autentiche del prestatore di servizi

27) *Cfr.* art. 10, comma 2, del d. lgs. 11/2010.

28) Cfr. Cass. Civ. 13 marzo 2023, n. 7214; Cass. Civ. 8 novembre 2023, n. 31136; Tribunale di Milano, 8 gennaio 2020, n. 79/2020; Collegio di Bari, Decisione n. 367 del 9 gennaio 2024.

29) *Cfr.* Collegio di Milano, Decisione n. 2006 del 15 febbraio 2024 – "*Nel caso di specie non si ravvisa alcun indice di spoofing particolarmente sofisticato considerato che il link contenuto nell'SMS truffaldino non aveva alcuna attinenza con l'intermediario convenuto né con altro istituto emittente di carte di pagamento e la telefonata ricevuta dal ricorrente – in base a quanto dal medesimo dichiarato in sede di denuncia – proveniva da un numero mobile non riconducibile all'intermediario*".

30) *Cfr.* Collegio di Milano, Decisione n. 1606 del 6 febbraio 2024; Collegio di Bologna, 14 febbraio 2024, n. 1934.

31) *Cfr.* Decisione ABF, Collegio di Milano, n. 1336 del 30 gennaio 2024.

di pagamento con le quali l'utente stesso è informato della installazione di una nuova utenza o dell'esecuzione di operazioni di pagamento ([32]);

- la ricezione da parte dell'utente di messaggi palesemente inattendibili e con indici di anomalia ([33]);

- la ricezione di telefonate e/o sms non riconducibili al prestatore di servizi di pagamento di riferimento dell'utente ([34]);

- la circostanza che l'utente abbia sostanzialmente ammesso (nel ricorso e nella denuncia all'Autorità competente) di aver "*abboccato*" al raggiro, comunicando al truffatore i codici di accesso alle funzionalità bancarie da remoto ([35]);

- la mancanza di sufficienti allegazioni fornite dall'utente in sede di disconoscimento, denuncia, reclamo o ricorso ABF in ordine alle caratteristiche della truffa subita, tale da indurre a ritenere che (a fronte di un ambiente presidiato dalla SCA del prestatore di servizi di pagamento) l'utente abbia disatteso gli obblighi di diligente custodia delle credenziali e cooperato affinché l'opera-

32) Sul punto, si richiama la Collegio di Bologna, decisione. n. 2593 del 28 febbraio 2024 laddove si legge che "*(...) Richiamate le norme, il Collegio con riferimento alle operazioni contestate rileva come l'intermediario produca la tracciatura dalla quale le operazioni risultano correttamente autenticate con doppio fattore, anche per quanto concerne l'attivazione alle ore 17:05:15 del 31 gennaio 2023, sull'utenza internet banking del ricorrente, di una nuova licenza ad operare, presumibilmente dal terzo truffatore sul proprio dispositivo mobile, per la quale si dovevano necessariamente inserire i dati (Password + OTP) ricevuti dal cliente. Il Collegio precisa, comunque, che la prova prodotta dall'intermediario non è di per sé sufficiente per attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento (cfr. Collegio di Coordinamento, decisione n. 22745/2019) e che è pertanto chiamato a valutare la sussistenza o meno della colpa grave del titolare dello strumento, in base a tutte le circostanze allegate. Alla luce delle circostanze esaminate nel caso in specie e della documentazione prodotta, in particolare la copia delle comunicazioni ricevute dal cliente via mail che lo informavano sia della installazione della nuova utenza, sia delle singole operazioni, il Collegio ritiene integrato tale requisito*".

33) *Cfr.* Collegio di Bologna, Decisione n. 1908 del 14 febbraio 2024; Collegio di Palermo, Decisione n. 702 del 15 gennaio 2024; Collegio di Bologna, Decisione n. 1080 del 24 gennaio 2024. A riguardo si richiama la sentenza n. 10743 emessa dal Tribunale di Napoli in data 30 novembre 2022 nella quale il Giudicante ha riconosciuto la colpa grave della parte attrice in riferimento ad una truffa perpetrata mediante invio di *c.d.* mail "*civetta*", rilevando che "*(...)* [n.d.r. previa ampia disamina della fattispecie all'uopo attenzionata] *3.4. Il caso in esame rientra dunque tra le ipotesi di phishing più comuni e ormai note alla clientela, anche senza particolari conoscenze informatiche, già all'epoca degli accadimenti. Le operazioni di bonifico di pagamento impartite sul conto dell'attore sono state autenticate regolarmente mediante i codici da egli stesso fomiti e non risulta ipotizzabile alcuna anomalia nel sistema di sicurezza della banca. L'aver abboccato alla e-mail palesemente ingannevole dei truffatori - sia per la sua riconoscibile anomala provenienza che per il suo contenuto - che non poteva essere confusa con un messaggio autentico della Banca costituisce certamente una grave colpa da parte dell'attore, tenuto conto altresì della professione (avvocato) e del grado di istruzione dello stesso. 3.5. La domanda risarcitoria va in definitiva rigettata. (...)*" (Tribunale di Napoli, sentenza n. 10743 del 30 novembre 2022).
Nella Decisione n. 8766 del 5 settembre 2023 il Collegio di Napoli, nella quale il Collegio, pur esprimendosi in merito ad una frode riconducibile al fenomeno *sms spoofing* (ossia la combinazione di smishing e spoofing), ed accogliendo parzialmente il ricorso del ricorrente accertando il c.d. concorso di colpa ai sensi dell'art. 1227 c.c. tra le parti, ha fornito chiare indicazioni in merito a quali possano essere gli indici di anomalia idonei a configurare la colpa grave dell'utente stesso. Testualmente si legge che: "*(...) Secondo l'orientamento condiviso dei Collegi (da ultimo, ABF Napoli, n. 3130/2023) nelle fattispecie di spoofing, data l'insidiosità del meccanismo di aggressione, consistente nell'invio del messaggio sms dall'utenza dell'intermediario, non è generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvengano indici di inattendibilità (quali ad es. evidenti errori grammaticali o sintattici) o di anomalia (quali ad es. l'invito a selezionare un link in nessun modo riferibile all'intermediario) che dovrebbero far allertare l'utente avveduto. In tale caso, potrà essere ravvisato un concorso di colpa tra le parti. Nel caso in esame, in effetti, il link indicato negli sms civetta non risulta univocamente riferibile all'intermediario; si osserva la ripetizione (di una parte) della denominazione dell'intermediario e la presenza di riferimenti ad una URL che non pare riconducibile allo stesso. Alla luce di tutto quanto sopra descritto, il Collegio ritiene che sussista un concorso di colpa tra le parti.*" (Collegio di Napoli, Decisione n. 8766 del 5 settembre 2023).

34) Sul punto, si richiama la Decisione ABF Prot. N. 0012883/23 del 19 dicembre 2023 del Collegio di Roma nella quale si legge che "*Il ricorso non merita accoglimento. (...). In sede di denuncia, la ricorrente ha dichiarato di aver ricevuto un sms da un mittente apparentemente riconducibile a un intermediario terzo, diverso dalla banca resistente; con tale messaggio, le veniva comunicato il blocco della carta per mancata sicurezza ai sensi della PSD2 e veniva indicato un link al fine di riattivare lo strumento; la cliente cliccava sul link e veniva indirizzata presso una pagina web nella quale veniva richiesto di riattivare le credenziali bancarie; a tal fine, compilava i campi fornendo le indicazioni richieste, senza tuttavia ultimare l'operazione; dopo pochi minuti, riceveva una telefonata e l'interlocutore, presentatosi come operatore bancario, invitava la cliente a ultimare la procedura; ultimava le operazioni e riceveva il codice OTP dell'intermediario; in seguito, riceveva sulla posta elettronica personale una mail dalla banca che la informava della sostituzione della propria mail con un'altra. 5. Alla luce della documentazione in atti risulta che la chat contenente il messaggio esca reca come mittente un intermediario terzo, il quale non è parte del presente procedimento. 6. Pertanto, il messaggio fraudolento non si è inserito in una conversazione contenente anche messaggi genuini. (...). 10. Si osserva altresì che la "contraffazione del mittente" è stata effettuata sull'ID mittente dell'intermediario emittente la carta, il quale non è parte del presente procedimento. 11. In casi caratterizzati dalla medesima dinamica, con messaggio civetta inviato da un mittente apparentemente riconducibile all'intermediario terzo che cura la gestione operativa della carta (il medesimo che viene qui in rilievo), estraneo al procedimento, il Collegio di Roma ha rilevato che "l'eventuale "contraffazione del mittente" (spoofing) è stata effettuata sull'ID dell'intermediario" diverso dall'intermediario resistente e ha respinto il ricorso (cfr. Collegio di Roma, decisione n. 5233/2023).*" (Collegio di Roma, Decisione Prot. N. 0012883/23 del 19 dicembre 2023, inedita; in senso conforme è la Decisione ABF del Collegio di Roma n. 5233/2023 del 26 maggio 2023).

35) Collegio di Torino, Decisione n. 1137 del 25 gennaio 2024.

zione fraudolenta potesse compiersi ([36]).

7. ***Aspettando PSD 3 ed il nuovo Regolamento PSR***

La forte spinta verso soluzioni di pagamento innovative e con regolamento istantaneo rappresenta una "priorità" del progetto di revisione della disciplina sui servizi di pagamento, ma al tempo stesso potrebbe accrescere il rischio di frodi ove non assistita da idonee misure a presidio della sicurezza delle operazioni di pagamento.

Nel progetto di revisione della disciplina PSD risulta fortemente avvertita la necessità di rafforzare la tutela degli utenti dal rischio di frode ([37]), ciò anche in ragione della considerazione che i processi di autenticazione forte non possono sempre elidere detto rischio ([38]) in quanto la maggior parte delle truffe di "ingegneria sociale" (*phishing*, *vishing*, *smishing*, *spoofing*) si verifica prima dell'applicazione della stessa SCA ([39]).

Assunto che la distinzione tra operazioni autorizzate e operazioni non autorizzate sia sempre più complessa da applicare nella pratica e che non sarebbe più possibile limitare i rimborsi alle sole operazioni non autorizzate ([40]), in sede europea si è proposta una nuova definizione di "autorizzazione" all'esecuzio-

36) Collegio di Bari, Decisione n. 917 del 22 gennaio 2024.

37) Nella Relazione che precede il testo della Proposta del Regolamento PSR della Commissione Europea, nella Sezione Contesto della Proposta – Motivi e obiettivi della proposta si legge che "*Nella strategia in materia di pagamenti al dettaglio si annunciava che "alla fine del 2021 la Commissione [avrebbe avviato] un riesame esaustivo dell'applicazione e dell'impatto della PSD2". Il riesame è stato debitamente effettuato, essenzialmente nel 2022, e ha portato alla decisione della Commissione di proporre alcune modifiche alla PSD2, per migliorarne il funzionamento.*". E ancora, nella successiva Sezione Risultati delle valutazioni *ex post*, delle consultazioni dei portatori di interessi e delle valutazioni di impatto – Valutazioni d'impatto, si legge "*La valutazione d'impatto ha evidenziato che, nonostante i risultati conseguiti dalla PSD2, il mercato dei pagamenti dell'UE presenta quattro problemi fondamentali: – i consumatori sono esposti al rischio di frode e non hanno fiducia nei pagamenti; (...). Tali problemi comportano, tra l'altro, le conseguenze seguenti: – gli utenti (in particolare consumatori, esercenti e PMI) continuano ad essere esposti al rischio di frode; (...). L'iniziativa si prefigge quattro obiettivi specifici, che corrispondono ai problemi individuati:*
1. *rafforzare la protezione degli utenti e la loro fiducia nei pagamenti;*
2. *migliorare la competitività dei servizi bancari aperti;*
3. *migliorare l'applicazione e l'attuazione negli Stati membri;*
4. *migliorare l'accesso (diretto o indiretto) dei prestatori di servizi di pagamento non bancari ai sistemi di pagamento e ai conti bancari. La valutazione d'impatto presenta un pacchetto di opzioni prescelte volte al conseguimento degli obiettivi specifici (l'elenco sotto riportato include sia le misure contenute nel presente regolamento che quelle della direttiva che lo accompagna): – per quanto concerne l'obiettivo specifico 1: una migliore applicazione dell'autenticazione forte del cliente, una base giuridica che preveda lo scambio di informazioni in materia di frodi e un obbligo a informare i clienti in merito alle frodi, l'estensione della verifica dell'IBAN a tutti i bonifici e l'inversione condizionata di responsabilità per le frodi che inducono a effettuare pagamenti erroneamente ritenuti come dovuti (authorised push payments); l'obbligo per i prestatori di servizi di pagamento di migliorare l'accessibilità dell'autenticazione forte del cliente per gli utenti con disabilità, le persone anziane e per chiunque altro incontri difficoltà nell'uso dell'autenticazione forte del cliente; misure per migliorare la disponibilità di contante; il miglioramento dei diritti dell'utente e delle informazioni fornitegli; (...)*".

38) Nella Relazione della Commissione al Parlamento Europeo, al Consiglio, alla Banca Centrale e al Comitato economico e sociale europeo sulla revisione della Direttiva (UE) 2015/2366, del 28 giugno 2023 - COM (2023) 365 *final* -, alla Sezione 3.4. ("*Sicurezza e prevenzione delle frodi*") si legge che: "*Nonostante i suoi ottimi risultati, l'SCA non contrasta tutti i tipi di frode. Di fronte all'emergere di nuovi tipi di frode, in particolare frodi di "ingegneria sociale", in cui i truffatori manipolano le vittime affinché rivelino le proprie credenziali o inviino fondi a un beneficiario illegittimo, per le quali l'SCA risulta scarsamente efficace, la Commissione propone nuove misure sia in materia di prevenzione delle frodi che di azioni per porvi rimedio.*".

39) *Cfr. Commission staff working document - impact assessment report* della Commissione Europea del 28 giugno 2023 – SWD (2023) 231 *final*, laddove nella Sezione "*New types of fraud not prevented by SCA*" si legge che "*There are still fraud-related problems, despite the success of SCA in reducing fraud. One of the drivers of these is the fact that fraudsters are constantly adapting their techniques to get around regulatory frameworks. Such techniques can involve illegal impersonation (e.g. a fraudster makes the payment instead of a genuine payer as a result of a cyberattack or theft of a payment instrument), or a criminal activity which occurs before the payment is made by a genuine payer. Such "pre-payment fraud" can take the form of invoice fraud (where invoices are intercepted and the merchant account number is substituted for that of the fraudster31), or more sophisticated "Authorised Push Payment" (APP) frauds involving social engineering of the payer through direct interaction (e.g. manipulation of the payer into believing s/he is dealing with a genuine payee or even with a bank representative). Cases of such APP fraud (phishing, vishing, smishing, spoofing etc.) cannot be tackled by SCA because, technically and legally, most of these fraudulent transactions have been authorised by the payer using SCA. The fraud is in fact taking place before SCA without the payer knowing that s/he is being defrauded. The consumer thinks in good faith that s/he is sending money to recipient X, whereas in reality s/he is sending money to a fraudster. According to the European Payments Council, social engineering attacks and phishing attempts are still increasing, often in combination with malware, with a shift from consumers, retailers, SMEs to company executives, employees (through "CEO fraud" or "impersonation fraud"), payment service providers (PSPs) and payment infrastructures and more frequently leading to APP fraud. These techniques have greatly evolved over the last years as the targets are users rather than technology (...)*".

40) Sul punto, si richiama il considerando 79 della proposta di Regolamento PSR nel testo emendato dal Parlamento Europeo ad aprile 2024, laddove si legge testualmente che "*Gli utenti di servizi di pagamento dovrebbero essere adeguatamente tutelati nel contesto delle cosiddette truffe di ingegneria sociale, nelle quali il truffatore manipola l'utente*
di servizi di pagamento affinché esegua una determinata azione, quale l'avvio di un'operazione di pagamento, o trasmetta le credenziali di sicurezza dell'utente di servizi di pagamento ai truffatori. Il numero di questo tipo di casi di "ingegneria

ne di operazione di pagamento che, per essere tale, deve essere stata resa con piena cognizione dall'utente ([41]) e senza alcuna manipolazione. In sostanza all'attuale ritmo binario previsto da PSD 2 (operazione autorizzata – operazione non autorizzata), potrebbe sostituirsi con il nuovo Regolamento PSR un ritmo a tre tempi in cui si distingua tra (i) operazione autorizzata, (ii) operazione autorizzata oggetto di frode, (iii) operazione non autorizzata.

Il legislatore europeo propone di disciplinare le operazioni oggetto di "*frode con furto di identità*" mediante il nuovo art. 59 della bozza di Regolamento PSR in cui si prevede che:

- qualora il consenso dell'utente sotteso all'autorizzazione di una operazione di pagamento sia stato "*manipolato da un terzo che ha finto di essere un dipendente del prestatore di servizi di pagamento del consumatore o qualsiasi altro ente pertinente di natura pubblica o privata utilizzando illecitamente il nome o l'indirizzo di posta elettronica o il numero di telefono di tale ente*", il prestatore di servizi di pagamento deve rimborsare il consumatore dell'intero importo dell'operazione autorizzata fraudolenta, ciò a condizione che il consumatore "*abbia tempestivamente segnalato la frode alla polizia e ne abbia informato il prestatore di servizi di pagamento*";

- ricevuta la segnalazione di una operazione autorizzata fraudolenta, unitamente alla denuncia effettuata alla polizia, il prestatore di servizi di pagamento avrà 10 giorni operativi per valutare se rimborsare il consumatore o, in alternativa, rigettare la richiesta di rimborso in quanto ritiene sussistenti "*ragionevoli motivi per sospettare una frode o una negligenza grave del consumatore*", dovendo in tale secondo fornire all'Autorità nazionale una informativa con la motivazione del rifiuto del rimborso;

- il diritto del consumatore al rimborso per le operazioni autorizzate fraudolente non sussiste nel caso in cui lo stesso abbia agito con dolo o colpa grave, ovvero qualora lo stesso consumatore si rifiuti di "*collaborare all'indagine del prestatore di servizi di pagamento o di fornire informazioni pertinenti in merito alle circostanze del furto di identità*";

- i prestatori di servizi di comunicazione elettronica sono tenuti a cooperare con i prestatori di servizi di pagamento per garantire la sicurezza e la riservatezza delle comunicazioni, anche per quanto concerne l'identificazione della linea chiamante e l'indirizzo di posta elettronica. Qualora siano stati informati della presenza di contenuti fraudolenti, i prestatori di servizi di comunicazione elettronica che non rimuovano tali contenuti saranno tenuti a rimborsare i prestatori di servizi di pagamento in relazione all'intero importo delle operazioni autorizzate fraudolente;

- i prestatori di servizi di comunicazione elettronica saranno chiamati ad avvertire i loro clienti in merito alle nuove forme di truffe on line, fornendo altresì indicazioni chiare su come individuare i tentativi fraudolenti ed in merito alle precauzioni da adottare per evitare di rimanere vittime di frodi;

- i prestatori di servizi di pagamento, i prestatori di servizi di comunicazione elettronica e i prestatori di servizi delle piattaforme digitali ([42]) dovranno disporre di tecniche di prevenzione e at-

sociale". è notevolmente aumentato negli ultimi anni. I casi di "spoofing" in cui i truffatori fingono di essere dipendenti del prestatore di servizi di pagamento di un cliente o di un'entità pertinente che potrebbe essere ragionevolmente collegata a una fonte fidata del cliente, quale una banca centrale o un'autorità governativa, e abusano del nome, dell'indirizzo di posta elettronica o del numero di telefono del prestatore di servizi di pagamento per conquistare la fiducia dei clienti e indurli a compiere alcune azioni sono purtroppo sempre più diffusi nell'Unione. Questi nuovi tipi di frode o "furto di identità" rendono meno netta la differenza esistente nella direttiva (UE) 2015/2366 tra operazioni autorizzate e non autorizzate. Le condizioni alle quali il cliente ha dato la sua autorizzazione all'esecuzione di un pagamento dovrebbero essere tenute in debita considerazione, anche da parte delle autorità giurisdizionali, per qualificare un'operazione come autorizzata o non autorizzata. L'autorizzazione di un'operazione può infatti essere stata concessa a seguito di una manipolazione che compromette l'integrità dell'autorizzazione. Pertanto non è più possibile limitare i rimborsi alle sole operazioni non autorizzate, come prevedeva la direttiva (UE) 2015/2366".

41) L'art. 3, punto 34 *bis* della proposta di Regolamento PSR nel testo emendato dal Parlamento Europeo ad aprile 2024, prevede che per "*autorizzazione*" deve intendersi un "*un permesso accordato in una procedura in cui l'utente di servizi di pagamento autentica una determinata operazione liberamente e con piena cognizione di tutti i fatti pertinenti*".
Il considerando n. 79 *bis* della proposta di Regolamento PSR nel testo emendato dal Parlamento Europeo ad aprile 2024, prevede che per "*Per quanto riguarda l'autorizzazione delle operazioni di pagamento, l'autorizzazione dovrebbe esprimere l'intenzione del pagatore fondata sulla piena cognizione dei fatti pertinenti, tra cui l'importo, il destinatario e la finalità dell'operazione. L'intenzione del pagatore, fondata sulla piena cognizione dei fatti pertinenti, al momento dell'operazione dovrebbe essere valutata conformemente al diritto nazionale*".

42) Nel considerando 81 *bis* del Regolamento PSR nel testo emendato dal Parlamento Europeo ad aprile 2024, si legge che "*Anche le piattaforme online possono contribuire all'aumento di casi di frode. Pertanto, e fatti salvi i loro obblighi a norma del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio2 (regolamento sui servizi*

vedi l'articolo online

tenuazione delle frodi in tutte le loro configurazioni, comprese le frodi che inducono a effettuare pagamenti erroneamente ritenuti come dovuti.

Anche nella proposta di Regolamento PSR in caso di "colpa grave" dell'utente lo stesso non avrebbe diritto al rimborso per le operazioni autorizzate fraudolente. Nella proposta di Regolamento PSR si riconosce che la colpa grave configura un comportamento che presenta un grado significativo di incuranza, che deve essere valutata sulla base di tutte le circostanze concrete e delle specifiche del diritto nazionale. Pur individuando talune casistiche sintomatiche di colpa grave ([43]), il legislatore europeo intenderebbe rimettere all'EBA l'adozione di specifici orientamenti relativi al concetto di colpa grave ([44]).

Sempre sul tema delle frodi nelle operazioni di pagamento di sicuro intesse risulta essere il parere dell'EBA di aprile 2024 ([45]) in cui la stessa Autorità ha rilevato più elevati tassi di frode per i bonifici istantanei e per le operazioni di pagamento transfrontaliere. Pur esprimendo apprezzamento per le azioni articolate nelle proposte della Commissione europea per la PSD3 e il Regolamento PSR, nonché alle disposizioni recentemente entrate in vigore con il Regolamento sui pagamenti istantanei 2024/886, EBA ritiene utili ulteriori azioni per mitigare il rischio di frodi ([46]).

digitali), essi dovrebbero essere ritenuti responsabili qualora la frode sia sorta come conseguenza diretta dell'utilizzo della loro piattaforma da parte di truffatori per ingannare i consumatori, se sono stati informati della presenza di contenuti fraudolenti sulla loro piattaforma e non li hanno rimossi".

43) Testualmente, al considerando 82 del Regolamento PSR nel testo emendato dal Parlamento Europeo ad aprile 2024, si legge che "*Per valutare l'eventuale negligenza o negligenza grave da parte dell'utente di servizi di pagamento, dovrebbero essere prese in considerazione tutte le circostanze. È opportuno che di norma le prove e il grado della presunta negligenza siano valutati sulla base del diritto nazionale. Tuttavia, mentre il concetto di negligenza implica la violazione di un dovere di diligenza, per negligenza grave si dovrebbe intendere qualcosa di più della semplice negligenza, ossia un comportamento che presenta un grado significativo di incuranza: ad esempio, effettuare un pagamento a un truffatore senza avere ragionevoli motivi per credere che il beneficiario a cui era indirizzato il pagamento sia legittimo, lasciare le credenziali usate per autorizzare un'operazione di pagamento vicino allo strumento di pagamento, in un formato aperto e facilmente individuabile da terzi, persuadere una banca a rimuovere il blocco posto a seguito di un avviso di frode, agendo sotto la guida di terzi sconosciuti, oppure consegnare a terzi uno smartphone sprovvisto di blocco schermo*"

44) *Cfr*. art. 59, par. 5 *quater* del Regolamento PSR nel testo emendato dal Parlamento Europeo ad aprile 2024.

45) EBA, *Draft EBA Opinion on new types of payment fraud and possible mitigants*, April 2024 (EBA-Op/2024/01).

46) EBA, *Draft EBA Opinion on new types of payment fraud and possible mitigants*, April 2024 (EBA-Op/2024/01) in cui si propongono ulteriori 5 misure per mitigare il rischio di frodi, ossia:

Il progetto di revisione della disciplina PSD ed il richiamato parere dell'EBA confermano come il tema delle operazioni oggetto di frode sia in divenire e che necessita di estrema attenzione, coinvolgendo gli interessi (e le responsabilità) dei prestatori di servizi di pagamento, degli utenti, nonché dei prestatori di servizi di comunicazione elettronica e delle piattaforme di commercio elettronico, tutti chiamati a cooperare nella lotta alle frodi.

- requisiti di sicurezza rafforzati per i prestatori di servizi di pagamento, ad integrazione del controllo IBAN/nome e delle misure di mitigazione delle frodi incluse nelle proposte PSD3/PSR, volti a rafforzare ulteriormente la procedura di autenticazione delle operazioni;
- l'adozione da parte dei prestatori di servizi di pagamento di un quadro di gestione del rischio di frode;
- la revisione della disciplina sulla responsabilità per le operazioni oggetto di frode, attraverso una corretta distinzione tra transazioni autorizzate e non autorizzate, nonché una precisazione del concetto di "colpa grave" dell'utente;
- una vigilanza rafforzata e armonizzata sulla gestione delle frodi, facendo leva anche sui dati sulle frodi già raccolti nell'ambito della PSD 2;
- requisiti di sicurezza adeguati per l'istituzione di un'unica piattaforma a livello europeo per la condivisione delle informazioni utili al fine di prevenire e individuare transazioni di pagamento potenzialmente fraudolente.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it