PHISHING E OPERAZIONI NON AUTORIZZATE: CHI SOPPORTA IL RISCHIO?

Onere della prova, allegazioni del cliente e limiti della responsabilità dell'intermediario tra ABF e giurisprudenza

VINCENZO LEMBO

SOMMARIO: 1. Premessa – 2. Il quadro normativo: equilibrio tra obblighi dell'utente e rischio d'impresa – 3. L'approccio dell'ABF – 3.1. Le operazioni "sotto dettatura" – 3.2. Lo spoofing e il problema del "messaggio civetta" – 3.3. Il vishing e l'usurpazione dell'identità telefonica – 3.4. Il Man in the Middle (MITM) e il Man in the Browser (MITB) – 4. Strong Customer Authentication – 5. Oltre la SCA: gli obblighi di prevenzione attiva dell'intermediario – 6. Colpa grave dell'utente e concorso di colpa – 7. Il ruolo delle allegazioni del cliente nel riparto della responsabilità – 8. Considerazioni conclusive.

1. Premessa.

Il phishing rappresenta oggi una delle principali fonti di contenzioso in materia di servizi di pagamento, ponendo al centro del dibattito una questione tutt'altro che semplice: chi sopporta il rischio della frode.

La crescente sofisticazione delle tecniche fraudolente – spesso realizzate mediante comunicazioni che simulano l'identità o i canali dell'intermediario – rende infatti difficile,

anche per un utente diligente, distinguere tra operazioni autentiche e fraudolente.[1]

[1] Il riferimento è alle principali evoluzioni del fenomeno del *phishing*, tra cui lo *spoofing* e il *vishing*, che si caratterizzano per la capacità di indurre il destinatario a ritenere genuina una comunicazione proveniente da soggetti apparentemente riconducibili all'intermediario, mediante la riproduzione di modalità comunicative tipiche dei canali ufficiali (SMS, email, telefonate).

In termini generali, il *phishing* si realizza attraverso l'invio di comunicazioni elettroniche ingannevoli da parte di soggetti terzi, finalizzate a indurre il destinatario ad aprire link o allegati malevoli, con conseguente possibile acquisizione indebita di credenziali o dati sensibili.

Più evoluta è la tecnica dello *spoofing*, che consiste nella manipolazione delle informazioni identificative del mittente di una comunicazione digitale. Nella forma più diffusa di *SMS spoofing* (o *smishing*), il messaggio fraudolento si inserisce talvolta all'interno di conversazioni già intercorse con l'intermediario, creando una continuità apparente con comunicazioni autentiche relative, ad esempio, all'invio di codici dispositivi o notifiche di servizio. Tale modalità è frequentemente idonea a generare un affidamento particolarmente intenso nel destinatario, rendendo più complesso distinguere la comunicazione fraudolenta da quelle legittime. Nella prassi decisionale dell'ABF, tali condotte sono state ricondotte alle ipotesi di frode connotate da maggiore sofisticazione, in ragione dell'elevato grado di mimetizzazione del messaggio (cfr. ABF, Collegio di Roma, decisione n. 481/2023).

Analoga logica si rinviene nel *vishing* (acronimo di *voice phishing*), che si realizza mediante contatto telefonico e che può assumere forme particolarmente insidiose nei casi di *caller ID spoofing*, in cui il numero visualizzato dal destinatario risulta coincidente con quello ufficiale dell'intermediario, inclusi i canali di assistenza o numeri verdi. In tali ipotesi, l'interlocuzione telefonica si presenta come proveniente da fonti apparentemente attendibili, contribuendo a rafforzare l'affidamento del cliente sulla genuinità della comunicazione (cfr. ABF, Collegio di Torino, decisione n. 5256/2023).

La combinazione delle diverse tecniche può dar luogo a schemi fraudolenti particolarmente efficaci, nei quali una comunicazione iniziale – apparentemente riconducibile all'intermediario – induce il cliente a compiere azioni dispositive o a inserire credenziali attraverso link malevoli, cui può seguire un ulteriore contatto telefonico volto a rafforzare l'inganno ed a sollecitare la comunicazione di codici dispositivi, spesso presentati come necessari per bloccare operazioni non autorizzate o per mettere in sicurezza il profilo utente. In tali contesti, la dinamica fraudolenta si fonda sulla progressiva costruzione di un affidamento ingannevole, che rende l'operazione percepita dal cliente come apparentemente urgente e legittima (cfr. ABF, Collegio di Torino, decisione n. 5256/2023).

Accanto a tali forme di inganno rientrano anche le tecniche di attacco di tipo *Man-in-the-Middle* (MITM), nelle quali il soggetto agente si interpone nella comunicazione tra utente e intermediario, intercettando e talvolta alterando i dati scambiati senza che le parti ne abbiano percezione. Una variante ulteriormente

In questo contesto, la tradizionale contrapposizione tra errore del cliente e responsabilità dell'intermediario tende progressivamente a sfumare. Il problema non è più soltanto stabilire se un'operazione sia stata formalmente autorizzata, ma piuttosto come distribuire il rischio della frode tra le parti.

Il quadro normativo, fondato sul d.lgs. n. 11/2010, sembra offrire una risposta chiara, ponendo a carico dell'intermediario un rigoroso onere probatorio. Tuttavia, la sua applicazione concreta da parte dell'Arbitro Bancario Finanziario (ABF) e della giurisprudenza restituisce un quadro più articolato, nel quale assume rilievo decisivo un accertamento in concreto che valorizza la condotta delle parti, anche sul piano processuale.

In tale prospettiva, il presente contributo si propone di analizzare il rapporto tra onere della prova e responsabilità nelle operazioni di pagamento non autorizzate, mettendo in luce come l'elaborazione dell'ABF e quella della giurisprudenza si muovano lungo direttrici in larga parte convergenti.

Particolare attenzione è dedicata al ruolo delle allegazioni del cliente, quale criterio interpretativo sempre più rilevante nel riparto della responsabilità, applicato tanto nella prassi dell'ABF quanto nella giurisprudenza anche più recente.

2. Il quadro normativo: equilibrio tra obblighi dell'utente e rischio d'impresa.

La disciplina della responsabilità per le operazioni di pagamento non autorizzate è contenuta principalmente nel d.lgs. 27 gennaio 2010, n. 11, che ha recepito in Italia la Direttiva

evoluta è rappresentata dal *Man-in-the-Browser* (MITB), in cui l'attacco avviene direttamente sul dispositivo dell'utente mediante l'installazione di un software malevolo, in grado di operare all'interno del browser e di modificare le operazioni in fase di esecuzione, senza che ciò sia immediatamente percepibile dal cliente. La giurisprudenza ha evidenziato come tali tecniche possano incidere significativamente sulla ricostruzione dell'evento, proprio in ragione della loro capacità di operare in modo non percepibile rispetto all'utente (cfr. Trib. Padova, sent. n. 2267/2023).

europea sui servizi di pagamento (PSD) e le successive modifiche della PSD2 (Direttiva UE 2015/2366).

Il sistema normativo è costruito intorno a un equilibrio, non privo di criticità, fra obblighi dell'utente e responsabilità dell'intermediario.

Da un lato, l'utente è tenuto a rispettare specifici obblighi di diligenza nella custodia e nell'utilizzo degli strumenti di pagamento. In particolare, egli deve utilizzare lo strumento conformemente alle condizioni contrattuali, proteggere le credenziali di sicurezza personalizzate e notificare senza indugio eventuali utilizzi non autorizzati (art. 7 d.lgs. 11/2010).

Dall'altro lato, a fronte del disconoscimento dell'operazione, è anzitutto onere dell'intermediario provare che l'operazione è stata *"autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure per la sua esecuzione o di altri inconvenienti"* (art. 10 d.lgs. 11/2010).

Tuttavia, tale onere non si esaurisce nella prova della regolarità tecnica dell'operazione.

Per andare esente da responsabilità, l'intermediario deve altresì dimostrare che l'operazione disconosciuta dal cliente è frutto di una condotta fraudolenta o dell'inadempimento degli obblighi ex art 7 d.lgs n. 11/2010 sorretto da dolo o colpa grave del cliente.

Tale passaggio assume carattere decisivo.

Il sistema non configura una responsabilità oggettiva dell'intermediario, ma neppure consente di addossare automaticamente il rischio al cliente: la ripartizione del rischio passa attraverso un accertamento in concreto della condotta delle parti.

In questa prospettiva, la giurisprudenza ha chiarito che il rischio di utilizzo indebito delle credenziali da parte di terzi rientra, in linea di principio, nell'area del rischio professionale

dell'intermediario, salvo che sia riconducibile a comportamenti dolosi o gravemente imprudenti del cliente.[2]

Ne deriva una conseguenza operativa di rilievo: la mera prova della corretta autenticazione non è sufficiente. L'intermediario deve quindi fornire elementi concreti idonei a dimostrare – anche in via presuntiva – che il cliente abbia violato in modo grave gli obblighi di custodia delle proprie credenziali.[3]

3. L'approccio dell'ABF.

È nella concreta applicazione di tali principi che emerge il contributo dell'Arbitro Bancario Finanziario, il quale ha progressivamente elaborato nelle proprie pronunce una serie di indicatori operativi utili a delimitare sia l'ambito della responsabilità dell'intermediario sia i confini della colpa grave dell'utente.

3.1. Le operazioni "sotto dettatura".

Una delle fattispecie più problematiche riguarda le operazioni eseguite personalmente dal cliente ma su indicazione del truffatore.

In tali ipotesi, la vittima viene contattata da un sedicente operatore e indotta a disporre un bonifico, spesso convinta di eseguire un'operazione di "sicurezza"; l'operazione risulta formalmente corretta ma sostanzialmente viziata dal raggiro.

In tale ambito, l'ABF adotta una lettura sostanzialistica del concetto di autorizzazione, valorizzando il grado effettivo di controllo dell'utente sull'operazione e distinguendo nettamente tra contributo pieno e contributo meramente esecutivo.

In questa direzione si colloca, tra le altre, la decisione del Collegio di Palermo n. 8840/2025[4], che esclude l'applicabilità

[2] Cass. Civ., Sez. 3, n. 13204 del 15.05.2023; Cass. Civ., Sez. 3, n. 3780 del 12.02.2024.

[3] ABF, Collegio di Coordinamento, Decisione n. 897 del 14/02/2014.

[4] ABF, Collegio di Palermo, Decisione n. 8840 del 02/10/2025.

della disciplina quando l'operazione sia integralmente riconducibile al pagatore (inserimento della disposizione e di tutti i fattori di autenticazione).[5]

Diversamente, qualora il contributo dell'utente sia solo parziale – ad esempio mediante la comunicazione di un codice OTP relativo ad un'operazione già predisposta dal frodatore – la transazione mantiene natura "non autorizzata", con conseguente applicazione della disciplina di tutela.[6]

3.2. Lo spoofing e il problema del "messaggio civetta".

Lo spoofing rappresenta una delle tecniche più insidiose, in quanto il messaggio fraudolento si inserisce all'interno di comunicazioni apparentemente riconducibili all'intermediario.

La prassi ABF richiede al cliente di fornire la prova dell'esistenza del messaggio ingannevole c.d. "civetta", potendo la mancata allegazione impedire la verifica dell'affidamento ingenerato.[7]

Anche in queste ipotesi, pur richiedendo al cliente un onere di allegazione minimo (quale la produzione del "messaggio civetta"), l'ABF mantiene ferma l'impostazione secondo cui la prova della responsabilità resta in capo all'intermediario, che deve dimostrare la regolarità tecnica dell'operazione e l'assenza di proprie carenze nei sistemi di sicurezza.

---

[5] In senso conforme, ABF, Collegio di Palermo, Decisione n. 8853 del 02/10/2025 e Decisione n. 8870 del 02/10/2025, le quali valorizzano il fatto che il cliente abbia volontariamente eseguito l'operazione, pur se indotto in errore dal raggiro.

[6] In tal senso, la decisione n. 8882/2025 del Collegio ABF di Bologna in cui si chiarisce che l'esclusione della PSD2 opera solo quando l'operazione sia eseguita per intero dal pagatore, mentre un apporto meramente parziale non è sufficiente a configurare un'autorizzazione in senso tecnico.

[7] ABF, Collegio di Palermo, Decisione n. 8852 del 02/10/2025, in cui è stato precisato che, nel caso di spoofing, la mancata allegazione, da parte del cliente, del messaggio "civetta", determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e se sia pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio.

3.3. Il vishing e l'usurpazione dell'identità telefonica.

Ulteriore evoluzione è rappresentata dal vishing, in cui il contatto avviene telefonicamente e il numero del chiamante appare coincidere con quello dell'intermediario o di autorità pubbliche, in ragione di tecniche di manipolazione dell'identificativo di chiamata (caller ID spoofing).

Il tratto caratterizzante di tali decisioni è la valorizzazione dell'affidamento dell'utente, che, in presenza di tecniche particolarmente insidiose, tende ad attenuare il giudizio di rimproverabilità e a condurre più frequentemente a soluzioni di concorso di colpa.

Il Collegio di Roma, con la decisione 10893/2025, osserva che tale situazione è da ricondursi *"alle truffe potenzialmente "sofisticate", equiparabile all'sms spoofed come fattispecie insidiosa in termini di supposta genuinità dei contatti"*, considerandola *"[…]come sintomo di una imperfezione nella sicurezza del sistema approntato dall'intermediario, in grado di giustificare un concorso di colpa fra le parti"*[8], mentre, con la decisione n. 8963/2025, individua la specifica responsabilità dell'intermediario per *"non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse chiamare la cliente con un numero riferibile all'intermediario medesimo"*.[9]

3.4. Il Man in the Middle (MITM) e il Man in the Browser (MITB).

Accanto alle tecniche di phishing e vishing, si collocano forme di frode tecnologicamente più invasive come gli attacchi "Man in the Middle" (MITM) e la loro variante "Man in the Browser" (MITB), caratterizzate dalla capacità di inserirsi in

[8] ABF, Collegio di Roma, Decisione 10893 del 11/12/2025.
[9] ABF, Collegio di Roma, Decisione n. 8963 del 13/10/2025.

modo occulto nella comunicazione tra l'utente e l'intermediario, alterandone il contenuto all'insaputa di entrambe le parti.[10]

Tali tecniche, pur incidendo sulla sicurezza delle operazioni, non implicano necessariamente una vulnerabilità intrinseca dei sistemi dell'intermediario, potendo realizzarsi anche attraverso la compromissione del solo dispositivo dell'utente o del canale di comunicazione, ferma restando la possibilità che, in concreto, possano concorrere ulteriori fattori di debolezza del sistema.

L'approccio dell'ABF in questi casi si mostra particolarmente protettivo nei confronti dell'utente. Con decisione n. 4654/2023, il Collegio di Torino, a fronte di un'operazione disconosciuta e ricondotta dall'intermediario stesso ad un malware presente sul dispositivo del cliente, ha disposto il rimborso integrale delle somme sottratte, affermando che la condotta della vittima di tale attacco non è, di regola, connotata da colpa grave, salvo la presenza di ulteriori elementi, quali, ad esempio, l'inerzia a fronte di evidenti anomalie del dispositivo.[11]

La natura di tali frodi incide significativamente sulla valutazione della responsabilità. A differenza del phishing tradizionale, nel quale può ravvisarsi un profilo di negligenza del cliente, negli attacchi MITB l'utente può operare in maniera del tutto corretta dal proprio punto di vista; ne consegue che la colpa grave del cliente è difficilmente configurabile e l'evento dannoso tende ad essere ricondotto nell'area del rischio professionale del prestatore di servizi di pagamento.

In questo contesto, l'onere probatorio a carico dell'intermediario ai sensi dell'art. 10 del d.lgs. 11/2010 assume un peso ancora maggiore: non è, infatti, sufficiente dimostrare la corretta autenticazione formale dell'operazione, poiché il

[10] Nell'attacco MITM, il malintenzionato intercetta la connessione tra l'utente e il server bancario, acquisendo e potenzialmente modificando le comunicazioni ed i dati in transito. La variante MITB risulta ancor più insidiosa, poiché opera direttamente sul dispositivo dell'utente (PC o smartphone) mediante l'installazione di un malware che consente di manipolare le operazioni bancarie senza che la vittima percepisca alcuna anomalia.

[11] ABF, Collegio di Torino, Decisione n. 4654 del 15/05/2023.

malware è in grado di catturare le credenziali e i codici dispositivi o, addirittura, di modificare i dati di un'operazione (come l'IBAN del beneficiario) successivamente all'autorizzazione dell'utente.

L'ABF, nella citata decisione, ha inoltre chiarito che non possono essere imputati al cliente obblighi di manutenzione informatica tali da integrare negligenza grave in caso di violazione.[12]

In linea con tale orientamento, occorre richiamare anche la sentenza del Tribunale di Torre Annunziata n. 1091/2025, la quale sottolinea come, in ragione del regime probatorio vigente, le fattispecie di attacco MITB comportino nella maggior parte dei casi l'obbligo per gli intermediari di risarcire i danni subiti dai clienti, risultando particolarmente gravoso dimostrare una colpa grave dell'utente che abbia operato senza percepire alcuna irregolarità.[13]

4. Strong Customer Authentication.

Un ruolo centrale è rappresentato dalla Strong Customer Authentication (SCA).[14]

La sua corretta applicazione costituisce un presupposto imprescindibile: in assenza di SCA, la responsabilità dell'intermediario tende, secondo l'orientamento applicativo, ad essere affermata con particolare rigore.

[12] Cit. ABF, Collegio di Torino, Decisione n. 4654 del 15/05/2023, in cui è stata respinta la difesa dell'intermediario che attribuiva la frode al mancato aggiornamento del sistema operativo, ritenendo che tale omissione non configuri né dolo né comportamento gravemente incauto dell'utente.

[13] Tribunale Di Torre Annunziata, Sentenza n.1091 del 02/05/2025.

[14] La definizione di autenticazione forte si rinviene nell'art. 1, lett. q-bis) d.lgs. n. 11/2010, ove si prevede che 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 (...)"*.

Come chiarito dalla decisione n. 10502/2025 del Collegio di Bologna, la prova dell'autenticazione forte costituisce un vero e proprio "prius logico" ai fini dell'esclusione della responsabilità dell'intermediario.[15]

Qualora, infatti, non fosse stata adottata dall'intermediario la detta autenticazione forte, il cliente ai sensi dell'art. 12 comma 2-bis del d.lgs. 11/2010 risponderebbe soltanto in caso di frode.

Un profilo frequentemente problematico riguarda il c.d. riutilizzo dei fattori di autenticazione nell'ambito della medesima sessione operativa.

In termini pratici, si tratta dei casi in cui l'utente, dopo aver effettuato l'accesso alla propria home banking mediante un primo fattore (ad es., biometrico), autorizza un'operazione di pagamento senza inserire nuovamente tutte le credenziali, ma attraverso un secondo passaggio semplificato (ad es., una notifica push).

Sul punto, la prassi applicativa[16] ritiene conforme agli standard di sicurezza il riutilizzo di un elemento di autenticazione già impiegato per l'accesso, purché l'operazione avvenga nell'ambito di una sessione unica, continua e adeguatamente protetta.[17]

Diversamente, non può ritenersi soddisfatto il requisito dell'autenticazione forte qualora i fattori utilizzati non siano effettivamente indipendenti.

È il caso, ad esempio, di sistemi nei quali le credenziali e i codici dispositivi vengono trasmessi attraverso il medesimo canale (come nel caso di password ed OTP inviati entrambi via SMS), così da ricadere nella medesima categoria del "possesso". In tali ipotesi, la SCA risulta in realtà inidonea a garantire il livello di sicurezza richiesto dalla normativa.[18]

[15] ABF, Collegio di Bologna, Decisione n. 10502 del 01/12/2025.

[16] In linea con gli orientamenti dell'EBA (Q&A 2018_4141).

[17] Cit. ABF, Collegio di Palermo, Decisione n. 8852 del 02/10/2025 la quale ammette il riutilizzo del fattore all'interno della medesima sessione operativa.

[18] ABF, Collegio di Bari, Decisione n. 1970 del 28/02/2023.

Sotto questo profilo, la prassi dell'ABF appare dunque improntata ad un rigore elevato nei confronti dell'intermediario, valorizzando la SCA non solo come requisito formale, ma come effettivo presidio sostanziale di sicurezza.

5. Oltre la SCA: gli obblighi di prevenzione attiva dell'intermediario.

L'orientamento dell'ABF evidenzia come l'obbligo dell'intermediario non si esaurisca nella predisposizione di sistemi di autenticazione forte ma si estenda a una gestione proattiva del rischio.

La Strong Customer Authentication, infatti, non rappresenta il punto di arrivo delle cautele esigibili, bensì il presupposto minimo della diligenza richiesta.[19]

In questa prospettiva, la diligenza dell'intermediario – da valutarsi secondo il parametro dell'"accorto banchiere" di cui all'art. 1176, comma 2, c.c. – si sostanzia nell'adozione di cautele ulteriori, non meramente standardizzate o automatizzate[20], ovvero nell'implementazione di un'effettiva attività di prevenzione attiva.

Assume, pertanto, rilievo decisivo la capacità dell'intermediario di individuare e reagire a indici di anomalia dell'operatività.

Un riferimento normativo in tal senso è rappresentato dal D.M. 30 aprile 2007, n. 112, adottato in attuazione della L. 166/2005 per la prevenzione delle frodi sulle carte di pagamento: l'art. 8 di tale decreto individua alcuni parametri di rischio, tra cui "sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento", l'esaurimento del plafond in 24 ore o richieste da Stati diversi in un breve arco

[19] Tribunale di Torre Annunziata, Sentenza n. 249 del 30/01/2025, secondo cui la SCA non costituisce il massimo delle misure tecnologicamente disponibili per contrastare fenomeni fraudolenti ma il livello minimo di protezione richiesto dal legislatore.

[20] Cit. Tribunale di Torre Annunziata, Sentenza n. 249 del 30/01/2025.

temporale[21]. Sebbene la norma si riferisca testualmente alle carte di pagamento, l'orientamento costante dell'ABF ne estende l'applicazione analogica anche ad altri strumenti, come i bonifici o altre disposizioni online, in ragione dell'unicità della ratio di protezione.[22]

Accanto a tali indicatori normativi, la prassi applicativa ha progressivamente elaborato un insieme più ampio di indici sintomatici di anomalia, tra cui: operazioni di importo elevato rispetto allo storico del cliente; pluralità di disposizioni concentrate in un arco temporale ristretto (soprattutto se istantanee); superamento dei limiti operativi contrattualmente previsti;[23] trasferimenti verso beneficiari nuovi o ubicati in aree geografiche inconsuete; operazioni effettuate da dispositivi o indirizzi IP non riconducibili alla normale operatività del cliente; ovvero sequenze operative incoerenti (ad esempio, modifica delle credenziali seguita immediatamente da disposizioni di pagamento di importo rilevante).

In presenza di tali indici, seguendo l'impostazione prevalente dell'ABF, la mancata attivazione di sistemi di blocco o verifica rafforzata può essere valutata, in concreto, come indice di una possibile inadeguatezza dei presidi organizzativi dell'intermediario, talora qualificata nelle decisioni come "difetto organizzativo" rilevante ai fini della responsabilità.[24] In tal senso si esprime, tra le altre, la decisione n. 8882/2025 del Collegio di Bologna, che ravvisa un concorso di colpa in capo

[21] Art. 8 Decreto del 30/04/2007, n. 112 – Min. Economia e Finanze, emanato in attuazione della L. 166/2005.

[22] ABF, Collegio di Bologna, Decisione n. 4737 del 23/04/2024.

[23] ABF, Collegio di Torino, Decisione n. 9714 del 09/10/2023 che ha dato continuità al principio espresso dal Collegio di coordinamento ABF, con pronuncia n. 16237/2018 secondo cui: *"L'operazione di pagamento con la quale viene superato uno dei limiti massimi contrattualmente fissati (c.d. plafond) per l'utilizzo dello strumento elettronico di pagamento, deve essere interamente restituita al cliente in quanto, se disconosciuta, difetta del suo consenso. A tale operazione non risulta applicabile nemmeno la franchigia eventualmente prevista dal contratto per i casi di furto o smarrimento in quanto trattasi di operazione di pagamento non autorizzata"*.

[24] ABF, Collegio di Roma, Decisione n. 1303 del 10/02/2023.

alla banca per non aver intercettato una sequenza anomala di bonifici istantanei ravvicinati.[25]

A tale impostazione si affianca, tuttavia, un diverso orientamento espresso dalla giurisprudenza di merito, secondo cui non è possibile individuare, nell'attuale quadro normativo, un obbligo generale in capo al prestatore di servizi di pagamento di monitorare le operazioni e di sospenderne l'esecuzione in presenza di anomalie. Secondo tale indirizzo, né l'art. 8 del d.lgs. n. 11/2010 né l'art. 70 della direttiva (UE) 2015/2366 prevedono un simile obbligo, trattandosi di disposizioni che attribuiscono al prestatore facoltà e strumenti operativi senza configurare un dovere giuridico di intervento preventivo; sulla scorta di tale orientamento, un simile obbligo finirebbe per attribuire all'intermediario un margine di discrezionalità eccessivamente ampio, con possibili ricadute negative sia sull'efficienza del sistema dei pagamenti sia sulla certezza dei rapporti.[26]

In tale contesto, assume inoltre rilevanza l'effettività dei sistemi di allerta: non appare sufficiente dimostrare l'invio di notifiche o SMS, ma risulta necessario che essi siano concretamente idonei a mettere in guardia l'utente. Anche in questo caso, l'ABF ritiene che l'adozione di un sistema di SMS alert non sia una mera opzione da proporre al cliente, ma una misura di sicurezza che l'intermediario dovrebbe adottare in modo generalizzato.[27]

In questa direzione si inseriscono i sistemi di verifica dell'identità dell'interlocutore (il c.d. "bollino di sicurezza"), che consentono di verificare in tempo reale se l'interlocutore telefonico sia un reale operatore bancario. La decisione n. 9180/2025 del Collegio di Bologna attribuisce rilievo decisivo a tale strumento, ritenendo che l'utente che ignori il "bollino di

[25] Cit. ABF, Collegio di Bologna, Decisione n. 8882 del 03/10/2025.

[26] Tribunale di Milano, Sez. 6 Civ., Sentenza n. 847/2023; conforme, Tribunale di Ancona, Sentenza n. 338/2024.

[27] Cit. ABF, Collegio di Roma, Decisione n. 1303 del 10/02/2023.

sicurezza", pur essendo nelle condizioni di verificarlo, incorra in una condotta connotata da significativa imprudenza.[28]

Nel complesso, è quindi ravvisabile una progressiva evoluzione dello standard di diligenza richiesto all'intermediario verso forme di diligenza tecnica rafforzata. La responsabilità dell'intermediario non si esaurisce nella conformità tecnica dei sistemi ma si estende alla loro effettiva capacità di prevenire e intercettare operazioni anomale, secondo una valutazione che deve essere condotta in concreto, alla luce delle specifiche circostanze del caso e del dibattito interpretativo in corso.

6. Colpa grave dell'utente e concorso di colpa.

La valutazione della colpa grave dell'utente rappresenta uno dei profili più delicati nella prassi applicativa e viene condotta dall'ABF alla luce delle circostanze concrete del caso, con particolare riguardo al grado di sofisticazione della tecnica fraudolenta utilizzata.

In tale prospettiva, un ruolo centrale è assunto dalle ipotesi di spoofing, nelle quali il messaggio o la comunicazione fraudolenta si inserisce in canali che, nella percezione dell'utente, appaiono riconducibili all'intermediario, come nel caso di SMS che si collocano all'interno di conversazioni già in essere con la banca.

In simili situazioni, l'ABF tende a escludere la colpa grave, riconoscendo come anche un utente diligente possa essere indotto in errore da modalità di aggressione particolarmente insidiose. In tal senso, il Collegio di Torino (decisione n. 12068/2024) ha evidenziato come l'inserimento del messaggio fraudolento in una conversazione preesistente con l'intermediario sia idoneo a generare un affidamento difficilmente superabile con l'ordinaria diligenza.[29]

[28] ABF, Collegio di Bologna, Decisione n. 9180 del 21/10/2025.
[29] ABF, Collegio di Torino, Decisione n. 12068/2024.

Diversamente, la colpa grave viene generalmente ravvisata nei casi in cui il cliente tenga condotte in contrasto con regole di prudenza comunemente riconosciute, quali, ad esempio, la comunicazione volontaria di codici di sicurezza in assenza di adeguate garanzie.

In questa direzione si colloca la decisione del Collegio di Coordinamento n. 9959/2024 che, pur riconoscendo, l'elevato grado di sofisticazione della tecnica utilizzata (SMS inserito nella chat dell'intermediario) ha ritenuto decisiva, ai fini dell'accertamento della colpa grave, la successiva inerzia dell'utente di fronte a segnali ulteriori di anomalia, quali il messaggio di attivazione della carta su wallet, non seguita da alcuna verifica presso l'intermediario.[30]

Tra questi due estremi si colloca un'ampia area intermedia, nella quale la prassi dell'ABF evidenzia, in numerosi casi, il ricorso allo strumento del concorso di colpa ex art. 1227 c.c., quale criterio di bilanciamento delle rispettive responsabilità.

Le decisioni più recenti dell'ABF offrono esempi rilevanti di tale approccio.

Un primo ambito applicativo è rappresentato dalle ipotesi di vishing con caller ID spoofing. In tali casi, i Collegi valorizzano, da un lato, l'affidamento ingenerato dalla apparente riconducibilità del contatto all'intermediario e, dall'altro, eventuali carenze nei presidi di sicurezza, giungendo frequentemente ad una ripartizione del danno.[31] [32]

Un secondo profilo concerne l'omessa rilevazione di anomalie operative. Il concorso di colpa viene frequentemente ravvisato quando l'intermediario non intercetti operazioni

[30] ABF, Collegio di Coordinamento, Decisione n. 9959/2024.

[31] Cit. ABF, Collegio di Roma, Decisione n. 8963 del 13/10/2025 che ha ravvisato una responsabilità concorrente della banca per non avere adottato misure idonee a impedire l'utilizzo fraudolento di numerazioni riconducibili alla propria utenza.

[32] Cit. ABF, Collegio di Roma, Decisione 10893 del 11/12/2025ì che ha qualificato il fenomeno come indice di vulnerabilità del sistema di sicurezza nel caso concreto.

significativamente difformi dal profilo del cliente per importo, frequenza o tempistica, a fronte, tuttavia, di una condotta dell'utente che abbia contribuito alla realizzazione della frode (ad esempio, mediante l'interazione con link fraudolenti). In tal senso, il Collegio di Bologna, con la decisione n. 8882/2025, ha ritenuto sussistente una responsabilità concorrente del PSP, quantificata nella misura del 30%, per non aver bloccato una sequenza anomala di bonifici istantanei ravvicinati – eseguiti nell'arco di pochi minuti su di un conto solitamente inattivo – valorizzando la mancata attivazione di adeguati presidi di controllo.[33]

Ulteriore elemento rilevante è rappresentato dalla reazione del cliente ai sistemi di alert o a segnali di anomalia evidenti e percepibili.[34]

L'ABF ritiene che l'attivazione di sistemi di alerting (SMS, notifiche push o e-mail) sia idonea, in linea di principio, a porre il cliente nella condizione di intervenire tempestivamente per limitare il pregiudizio; ne consegue che la mancata reazione a tali segnalazioni può essere valorizzata, in concreto, quale possibile indice di negligenza dell'utente.[35] Tale rilievo, tuttavia, presuppone che gli alert siano effettivamente idonei a consentire un intervento utile, dovendosi escludere la loro rilevanza nei casi in cui la sequenza fraudolenta si sviluppi in un arco temporale talmente ristretto da rendere impossibile una reazione tempestiva da parte dell'utente.[36]

Un ulteriore profilo, in parte contiguo, riguarda la capacità del cliente di percepire e reagire a segnali di anomalia già nella fase

[33] Cit. ABF, Collegio di Bologna, Decisione n. 8882 del 01/10/2025.

[34] In giurisprudenza, Tribunale di Terni, Sentenza n. 832 del 28/10/2024, che ha evidenziato come una risposta tardiva o inadeguata a segnali di anomalia possa rilevare ai fini del concorso di colpa: in particolare, il Tribunale di Terni ha ricondotto la mancata tempestiva attivazione del cliente – a fronte di notifiche relative ad operazioni in corso – a una condotta negligente idonea a giustificare una riduzione del risarcimento ai sensi dell'art. 1227 c.c., pur senza interrompere il nesso causale tra l'evento e il danno

[35] ABF, Collegio di Roma, Decisione n. 2881 del 05/03/2024.

[36] ABF, Collegio di Palermo, Decisione n. 3649 del 17/04/2023.

prodromica alla frode, quali, ad esempio, la presenza di link non riconducibili ai domini ufficiali dell'intermediario o richieste atipiche di comunicazione di credenziali. Anche in tali ipotesi, la valutazione del comportamento dell'utente viene condotta in concreto, potendo la mancata percezione di anomalie evidenti essere valorizzata quale indice di comportamento gravemente imprudente.[37]

Infine, il concorso di colpa viene riconosciuto anche nelle ipotesi in cui il cliente abbia cooperato attivamente alla realizzazione della frode – ad es., mediante comunicazione di codici o installazione di applicazioni di controllo remoto – qualora tale condotta si inserisca in un contesto connotato da elevata insidiosità.

In questo quadro, la prassi dell'ABF tende a distinguere tra frodi caratterizzate da modalità elementari, nelle quali la violazione delle regole di prudenza può integrare colpa grave, e frodi connotate da elevata sofisticazione, nelle quali l'affidamento ingenerato dalla apparente genuinità della comunicazione impedisce di attribuire rilievo esclusivo alla condotta del cliente.[38]

In simili ipotesi, anche a fronte di una cooperazione attiva del cliente, la condotta di quest'ultimo non viene generalmente ritenuta, di per sé, sufficiente a escludere la responsabilità dell'intermediario, potendo piuttosto concorrere con eventuali carenze nei presidi di sicurezza o nei sistemi di controllo.[39] Un analogo approccio si rinviene nelle fattispecie di caller ID spoofing, nelle quali la simulazione dell'identità dell'intermediario è ritenuta idonea a incidere in modo significativo sulla capacità di discernimento dell'utente. Anche in tali casi, pur in presenza di profili di imprudenza, la condotta del cliente viene valutata nel contesto complessivo della

[37] ABF, Collegio di Roma, Decisione n. 5950 del 16/05/2024.

[38] Cit. ABF, Collegio di Bologna, Decisione n. 10502 del 01/12/2025.

[39] ABF, Collegio di Bari, Decisione n. 8939 del 12/09/2023.

vicenda, con frequente ricorso allo schema del concorso di colpa.[40]

Nel complesso, la prassi dell'ABF consente di individuare un orientamento nel quale il concorso di colpa assume un ruolo centrale nel bilanciamento delle rispettive responsabilità alla luce delle peculiarità del caso concreto, consentendo di modulare la responsabilità in modo coerente con il grado di diligenza delle parti e con l'effettiva capacità dei sistemi di prevenzione di intercettare l'evento fraudolento.

7. Il ruolo delle allegazioni del cliente nel riparto della responsabilità.

Il quadro normativo pone, come visto, in capo al prestatore di servizi di pagamento un rigoroso onere probatorio. Tuttavia, sia nella giurisprudenza di merito sia nella prassi dell'ABF, si va affermando un criterio interpretativo sempre più rilevante: la valorizzazione del comportamento del cliente non solo sul piano materiale, ma anche su quello processuale ed allegatorio.

Si delinea, in particolare, una forma di cooperazione narrativa, il cui mancato assolvimento può assumere rilievo sul piano della valutazione della colpa grave, pur senza determinare un'inversione dell'onere della prova.

Un esempio significativo di questa tendenza è offerto dalla sentenza della Corte d'Appello di Milano del 13 marzo 2026, n. 696.

In tale pronuncia, pur riconoscendo ai log di tracciamento prodotti dalla banca la natura di riproduzioni informatiche ai sensi dell'art. 2712 c.c. idonee a provare la regolarità tecnica delle operazioni, la Corte ha attribuito rilievo al deficit allegatorio della parte attrice. I giudici hanno osservato come l'assenza di una "ricostruzione, anche solo ipotetica, delle modalità della frode dedotta" costituisca un elemento rilevante: la valutazione della condotta del cliente è stata condotta anche

[40] ABF, Collegio di Torino, Decisione n. 3898 del 24/04/2023.

alla luce della mancanza di una narrazione alternativa plausibile, in presenza della prova offerta dall'intermediario circa l'affidabilità dei propri sistemi.[41]

Un analogo orientamento emerge con chiarezza nella prassi dell'ABF.

In diverse decisioni i Collegi hanno affermato che la mancata o generica allegazione delle circostanze della frode può, in determinate circostanze, essere valorizzata quale indice presuntivo, unitamente ad altri elementi, ai fini della valutazione della condotta del cliente, in quanto impedisce di verificare la plausibilità della dinamica prospettata e, al contempo, ostacola l'esercizio del diritto di difesa dell'intermediario.[42] È stato rilevato che un disconoscimento meramente formale e non circostanziato non è sufficiente, dovendo il ricorrente fornire almeno gli elementi fattuali rientranti nella propria sfera di conoscenza utili a spiegare l'accaduto.[43]

In tale prospettiva si colloca anche la richiesta, ricorrente nella prassi ABF, di produrre il c.d. "messaggio civetta" nelle ipotesi di spoofing: come evidenziato (v. par. 3.2), la mancata allegazione di tale elemento può impedire di apprezzare il grado di insidiosità della frode e, quindi, di valutare l'affidamento ingenerato nel cliente.

La valorizzazione del profilo allegatorio trova, tuttavia, un limite nei principi affermati dalla Corte di Cassazione con l'ordinanza n. 26916 del 26 novembre 2020, secondo cui non può pretendersi dal cliente l'allegazione di circostanze che non rientrano nella sua sfera di conoscibilità, né può trarsi da tale mancanza alcun elemento a suo carico.

Il principio espresso dalla Corte è particolarmente rilevante, poiché evita che l'onere di cooperazione narrativa si traduca in un'inversione dell'onere della prova. In particolare, la Corte ha

[41] Corte di Appello di Milano, Sez. I, Sentenza n. 696 del 13/03/2026.

[42] ABF, Collegio di Palermo, Decisione n. 6565 del 27/06/2023.

[43] ABF, Collegio di Torino, Decisioni n. 4962 del 22/05/2023 e n. 3900 del 24/04/2023.

chiarito che non può essere considerata significativa – né tantomeno sintomatica di colpa grave – la mancata allegazione di eventi che il cliente non ha percepito né può ragionevolmente ricostruire, quali, ad esempio, il furto o lo smarrimento delle credenziali quando tali fatti non si siano verificati o non siano stati percepiti come tali.[44] Diversamente opinando, si finirebbe per imporre al cliente un onere di ricostruzione tecnica della frode che esula dalle sue capacità e che appartiene, invece, alla sfera di controllo dell'intermediario.

Ne consegue che il deficit allegatorio assume rilievo solo con riferimento a circostanze che rientrano nella diretta esperienza del cliente – quali le modalità di ricezione di comunicazioni sospette, il contenuto di eventuali contatti con i truffatori o la percezione di anomalie – mentre non può essere valorizzato con riguardo a profili che attengono all'origine tecnica dell'evento fraudolento o a fatti rimasti del tutto ignoti alla vittima.

Nel quadro delineato, una narrazione lacunosa o incoerente su aspetti che solo il cliente può conoscere può concorrere, unitamente ad altri elementi, alla valutazione di una condotta incauta, nei limiti delle circostanze concretamente accertate, tale da integrare la colpa grave, soprattutto quando la banca ha dimostrato di aver messo a disposizione sistemi di allerta che avrebbero dovuto suscitare una reazione.[45]

Nel complesso, la prassi ABF e la giurisprudenza di merito appaiono dunque convergere verso un modello di accertamento nel quale dimensione tecnica e dimensione fattuale risultano strettamente integrate e nel quale il contributo allegatorio del cliente – lungi dal costituire una inversione dell'onere probatorio

[44] Cass. Civ., Sez. 6, n. 26916 del 26/11/2020, in cui viene affermato che resta *"irrilevante la mancata specifica di circostanze quali furto o smarrimento di carta o codici che, peraltro, non è dato sapere come avrebbero potuto conoscersi, e dunque allegarsi, dalla persona offesa, ove non accadute"*.

[45] In tal senso, nella Decisione n. 939/2023 il Collegio ABF di Milano ha ritenuto che l'assenza di una ricostruzione credibile fosse elemento idoneo a escludere l'esistenza di una "ragionevole alternativa" ad una condotta gravemente imprudente.

di legge – assume un ruolo rilevante sul piano della valutazione complessiva della vicenda e della ripartizione del rischio.

8. Considerazioni conclusive.

Le considerazioni svolte evidenziano come il tema della responsabilità per operazioni di pagamento non autorizzate si stia progressivamente ridefinendo attorno a due direttrici principali: da un lato, l'effettività dei presidi tecnici ed organizzativi predisposti dall'intermediario; dall'altro, la capacità del cliente di offrire una ricostruzione coerente e plausibile della vicenda.

Sul versante dell'intermediario, la centralità della Strong Customer Authentication non esaurisce il contenuto dell'obbligazione di sicurezza. Assume rilievo crescente la capacità del sistema di intercettare e gestire situazioni anomale attraverso strumenti dinamici, quali meccanismi di alerting, sistemi di blocco e modelli di analisi del comportamento dell'utente. Non è sufficiente, in altri termini, che il sistema sia formalmente conforme agli standard normativi: esso deve dimostrarsi concretamente idoneo a prevenire o contenere il rischio di operazioni fraudolente.

Sul versante del cliente, la condotta non può essere valutata in termini meramente formali, ma deve essere apprezzata nella sua dimensione complessiva, che include anche il profilo allegatorio. Come emerso dall'analisi comparata della giurisprudenza e della prassi ABF, non si tratta di imporre la dimostrazione di fatti negativi né di introdurre indebite inversioni dell'onere probatorio, bensì di riconoscere che la ricostruzione dell'accaduto costituisce una forma di cooperazione essenziale, nei limiti dei fatti effettivamente conoscibili dal cliente, secondo quanto chiarito dalla Corte di Cassazione.[46]

[46] Cit. Cass. Civ., Sez. 6, n. 26916 del 26/11/2020.

In questa prospettiva, il giudizio tende a strutturarsi come un confronto tra la tenuta del sistema predisposto dall'intermediario e la coerenza della ricostruzione offerta dal cliente. Quando il primo risulti adeguato e la seconda manchi o si presenti lacunosa, ciò può incidere sulla valutazione complessiva della condotta dell'utente e della riconducibilità dell'evento alla sua sfera di responsabilità, ferma restando la necessità di un accertamento in concreto; viceversa, in presenza di carenze nei presidi o di anomalie non intercettate, la responsabilità dell'intermediario non può ritenersi esclusa, anche a fronte di condotte non pienamente avvedute del cliente, specie ove la frode si caratterizzi per modalità particolarmente insidiose.

Ne emerge un quadro nel quale la ripartizione del rischio non è affidata a schemi rigidi, ma alla valutazione della condotta delle parti e dell'effettiva capacità dei sistemi di prevenzione di governare il rischio tecnologico.