DB non solo diritto bancario

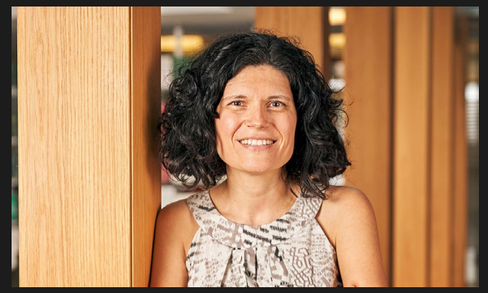
leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Le frodi informatiche negli ultimi orientamenti dell'ABF

Novembre 2025

Simona Daminelli, Partner, La Scala Società tra Avvocati
Francesca Fiorito, Associate, LegalMind



Simona Daminelli, Partner, La Scala Società tra Avvocati

Francesca Fiorito, Associate, LegalMind

Simona Daminelli

È Partner de La Scala Società tra Avvocati dal 2009 e opera nel team Contenzioso Bancario. Esperta di diritto bancario, assiste la clientela nelle fasi giudiziali e stragiudiziali di recupero del credito, nei procedimenti di mediazione e negoziazione assistita, nonché nella gestione del contenzioso bancario. Ha sviluppato una particolare competenza in materia di anatocismo, trasparenza bancaria, di legge anti-usura e nelle controversie attinenti la circolazione dei titoli di credito e i rapporti contrattuali di garanzia. È autrice di articoli e approfondimenti in tema di diritto bancario per le maggiori testate di settore e partecipa come relatrice a convegni in materia di contenzioso bancario.

1. I numeri e la normativa

Il fenomeno delle frodi informatiche è sempre di grande attualità e negli ultimi anni non conosce tregua. Come noto, le frodi hanno avuto un incremento esponenziale a partire dall'epoca covid, durante la quale si è dovuto ricorrere necessariamente ad un maggiore utilizzo della moneta elettronica e, in generale, di Internet, prestando così il fianco a più ampie possibilità di truffa. Le frodi informatiche, peraltro, sono in continua evoluzione e ne vengono quotidianamente ideate di sempre più sofisticate ed articolate, grazie alle continue innovazioni tecnologiche e, da ultimo, all'impiego dell'intelligenza artificiale.

Come emerge dai dati pubblicati dalla Polizia Postale Italiana, dal 2018 al 2022, non solo i casi di frode sono raddoppiati, ma soprattutto le somme di denaro trafugate sono cresciute in maniera esponenziale, attestando così la sempre maggiore abilità dei truffatori.

Ad agosto 2025, Banca d'Italia ha pubblicato il "Rapporto sulle operazioni di pagamento fraudolente in Italia nel 2° semestre 2024", nel quale è stato analizzato l'andamento delle frodi nei pagamenti digitali. In particolare, da tale documento emerge che sono in calo le truffe legate ai pagamenti con carte ed ai prelievi presso gli sportelli ATM, mentre è aumentato il tasso di frode legato all'uso dei bonifici istantanei. In generale, le operazioni di pagamento a distanza sono più esposte al rischio di frodi e, soprattutto, è stata riscontrato una maggiore incidenza delle frodi per le operazioni transfrontaliere rispetto a quelle nazionali.

Inoltre, Banca d'Italia ha evidenziato come, nei pagamenti con carte e moneta elettronica e nei prelievi ATM, sono più diffuse le operazioni effettuate senza il consenso del legittimo titolare (c.d. operazioni "non autorizzate" o "disconosciute"), mentre per i bonifici è più significativa l'ipotesi della "manipolazione del pagatore" che ricomprende tutti i casi in cui il cliente è indotto dal frodatore ad eseguire un pagamento, sfruttando informazioni raccolte con le tecniche di social engineering e facendo leva soprattutto sulle emozioni.

L'incremento delle frodi ha richiesto un intervento legislativo a livello nazionale e comunitario, che inizialmente si è, però, rivelato carente. Si consideri, infatti, che la prima direttiva europea sui sistemi di pagamento (cosiddetta PSD) risale al 2007 ed è stata recepita nel nostro ordinamento soltanto nel 2010 con il decreto legislativo numero 11. In altre parole, nel momento in cui è entrata in vigore la norma era

vedi l'articolo online

già vecchia, considerato che nel frattempo si erano sviluppate nuove frodi. Da qui la necessità di emanare una seconda direttiva (c.d. PSD 2) nel 2015. Il pregio principale di quest'ultima è stata l'introduzione di un sistema di autenticazione più rigoroso, il cosiddetto *strong customer authentication* (SCA), che si basa sull'utilizzo di una combinazione di fattori individuati sulla base di tre elementi indipendenti tra loro, ossia quelli della conoscenza, dell'inerenza e del possesso. Per avere un'autenticazione forte è necessario che il prestatore di servizi chieda l'utilizzo da parte del cliente di almeno due di questi fattori. Come rilevato anche da EBA, le transazioni autenticate con SCA presentano un numero inferiore di frodi rispetto a quelle che non richiedono l'autenticazione forte.

Attualmente sono in fase di avanzamento nel processo legislativo europeo le proposte di una terza direttiva (PSD 3) e di un regolamento sui servizi di pagamento (PSR), che potrebbero entrare in vigore nel 2026 e che mirano a rafforzare i sistemi di sicurezza dei pagamenti elettronici e digitali, introducendo norme più rigorose, nonché a migliorare la protezione dei consumatori.

2. Tipologie di frodi

Negli ultimi anni, la digitalizzazione dei servizi finanziari ha portato con sé un notevole miglioramento dell'efficienza e della comodità per gli utenti. Ma ogni innovazione, si sa, apre anche nuove porte all'ingegno criminale. Come detto, infatti, le frodi informatiche legate ai sistemi di pagamento sono oggi un fenomeno sempre più sofisticato e insidioso, capace di colpire anche i più attenti. Per comprendere appieno l'evoluzione del fenomeno, è utile passare in rassegna le principali tipologie di truffa online, analizzando le modalità con cui i malintenzionati riescono a sfruttare le vulnerabilità del sistema e quelle umane.

a. Phishing: la truffa "classica"

Tra le tecniche più diffuse, il *phishing* resta un evergreen della frode digitale. È un inganno costruito ad arte per spingere gli utenti a rivelare dati sensibili – numeri di conto, password, codici di accesso – attraverso canali che imitano alla perfezione le comunicazioni ufficiali di banche e istituti di pagamento. Un' e-mail dall'aspetto credibile, un link apparentemente innocuo o un messaggio su WhatsApp: basta un clic sbagliato per cadere nella rete.

Il Collegio di Coordinamento dell'Arbitro Bancario Finanziario (decisione n. 3498/12) ha definito questa pratica una frode "classica": un tranello che, con un minimo di attenzione, il cliente può – e dovrebbe – evitare, anche grazie alle campagne di sensibilizzazione ormai diffuse da tempo.

Oggi, però, il *phishing* si declina in varianti sempre più insidiose: lo *smishing*, veicolato tramite SMS, e il *vishing*, che sfrutta il contatto telefonico. Spesso le due modalità si combinano: prima un messaggio d'allarme, poi la telefonata del "finto operatore" che convince la vittima a fornire dati personali o ad autorizzare operazioni di pagamento.

b. Spoofing e Boxing

Se il *phishing* si basa sull'imitazione, lo *spoofing* va oltre: altera persino l'origine della comunicazione. In pratica, il truffatore modifica le informazioni del mittente per far sembrare che il messaggio o la chiamata provengano davvero dalla banca o da un interlocutore affidabile.

Le due forme più diffuse sono l'*SMS spoofing* e il *vishing caller ID spoofing*. Nel primo caso, le comunicazioni fraudolente possono perfino mescolarsi ai messaggi autentici dell'intermediario, all'interno dello stesso canale di conversazione. Nel secondo, il numero visualizzato sul display del telefono è falsificato, rendendo quasi impossibile distinguere la truffa dalla realtà.

Esiste poi una variante evoluta del classico *vishing*, denominata *Boxing*: in tal caso, il truffatore intercetta la carta di pagamento direttamente nella cassetta postale del titolare, insieme ai dati personali del cliente. Da solo, questo passaggio non basta a compromettere lo strumento: servono anche le credenziali per autorizzare i pagamenti, che il frodatore ottiene sfruttando un altro potente alleato: il social engineering.

In questa variante evoluta del classico *vishing*, il truffatore si finge un operatore dell'istituto finanziario, sfruttando informazioni riservate per guadagnare la fiducia della vittima. Le telefonate sembrano legittime, i messaggi convincenti e il cliente, inconsapevolmente, fornisce PIN e codici temporanei, completando il puzzle del reato.

Il risultato è un perfetto connubio tra tecnica e psicologia: la carta fisica e i dati rubati durante la spe-

vedi l'articolo online

dizione, combinati con le credenziali ottenute tramite inganno, permettono al criminale di effettuare prelievi o acquisti non autorizzati. Non sorprende che, in tali casi, la responsabilità sia stata ripartita tra la vittima e l'istituto, a testimonianza della complessità di queste truffe ibride: "*In particolare, dalla descrizione degli eventi richiamati dalla ricorrente e pedissequamente riportati nel verbale di denuncia prodotto agli atti, risulta la rivelazione al truffatore delle credenziali statiche, nonché di quelle dinamiche ricevute via sms, attraverso le quali l'artefice della truffa in possesso del bancomat rubato durante la sua spedizione ha potuto attivare la carta di debito ed effettuare i prelievi disconosciuti. […] Passando all'analisi in ordine alla sussistenza della colpa grave della ricorrente, il Collegio, premesso che a tal fine nessun rilievo assume la circostanza, evidenziata dall'intermediario, che le credenziali della carta erano in possesso del figlio della ricorrente, evidenzia tuttavia che quest'ultima dichiara sia in sede di denuncia, sia in sede di repliche di aver seguito, per il tramite del figlio medesimo, le indicazioni del sedicente operatore telefonico, digitando il link e inserendo le credenziali statiche e dinamiche, di talché, richiamando il proprio orientamento, ritiene che nel caso di specie sia ravvisabile una ripartizione di responsabilità al 50% fra entrambe le parti coinvolte*"(ABF Collegio di Bari n. 4048/2022).

Oltre a sottrarre informazioni riservate, queste tecniche possono servire anche a installare malware sui dispositivi delle vittime, dando ai criminali l'accesso remoto a dati e transazioni. Un inganno nel segno dell'illusione: far credere di essere chi non si è.

c. SIM Swap: il furto d'identità che parte dal telefono

Tra le frodi in crescita più rapida troviamo il *SIM Swap* (o *SIM Scam*), una truffa che unisce abilità informatica e social engineering. Il truffatore si procura una copia del documento d'identità della vittima – magari tramite un software "spia" – e si presenta al gestore telefonico fingendosi il legittimo titolare.

Ottiene così un duplicato della SIM, intercettando chiamate, messaggi e, soprattutto, le *OTP* (One-Time Password) necessarie per confermare le operazioni bancarie. Da quel momento, la vittima è di fatto tagliata fuori dal proprio numero di telefono, mentre il criminale ne sfrutta l'identità digitale.

d. Man in the Browser e Man in the Middle

Più sofisticate ma altrettanto pericolose sono le truffe note come *Man in the Browser (MITB)* e *Man in the Middle (MITM)*. Nel primo caso, un malware infetta il browser del computer della vittima, alterando le operazioni bancarie senza che l'utente se ne accorga: la pagina web sembra autentica, ma in realtà i dati viaggiano verso mani sbagliate. Nel secondo, l'attacco avviene "in mezzo" alla comunicazione: l'hacker si interpone tra due interlocutori, fingendosi l'uno con l'altro e riuscendo così a intercettare – o addirittura modificare – i messaggi scambiati.

Sono trappole invisibili, difficili da riconoscere anche per gli utenti più esperti, che dimostrano quanto la sicurezza informatica sia oggi un terreno in continua evoluzione, dove la consapevolezza resta la prima forma di difesa.

3. L'orientamento giurisprudenziale

La giurisprudenza sia di merito che di legittimità non è purtroppo univoca in tema di frodi informatiche, anche in ragione dell'elevata sofisticazione dei nuovi schemi fraudolenti, che rendono sempre più complessa l'individuazione tempestiva delle condotte illecite e la definizione di criteri applicativi omogenei.

Questo ha inizialmente spinto i giudici a valutare con particolare rigidità la responsabilità degli istituti di credito, al fine di garantire la fiducia dei clienti nella sicurezza del sistema. In particolare, tramite alcune decisioni della Suprema Corte intervenute tra il 2016 e il 2018 (v. Cassazione nn. 2950/2017, 10638/2016 e 9158/2018), è stata attribuita alle banche una sorta di responsabilità oggettiva: in altre parole, il solo verificarsi della frode, comportava automaticamente la responsabilità risarcitoria della banca, poiché l'impatto dell'operazione illecita veniva ricondotto nell'area di rischio professionale del prestatore di servizi di pagamento, quale soggetto "forte" e strutturalmente in grado di adottare misure adeguate per accertare la reale volontà del cliente nell'autorizzare le operazioni.

In una fase successiva, la giurisprudenza ha adottato un approccio meno rigoroso nella valutazione della prova liberatoria offerta dal prestatore di servizi, riconoscendo maggiore rilevanza sia all'adozione di sistemi di sicurezza adeguati, sia all'eventuale condotta negligente dell'utente vittima della frode.

In tal senso, per prima la Corte di Cassazione con ordinanza 13 marzo 2023, n. 7214, ha escluso la responsabilità della banca in un caso in cui il cliente aveva mal custodito i propri codici personali, digitandoli a seguito di una mail fraudolenta. Pochi mesi dopo, la Corte d'Appello di Milano, con decisione

13 novembre 2023, n. 3330, ha seguito tale strada escludendo la responsabilità del prestatore di servizi, atteso che "*la valutazione complessiva delle circostanze esposte porta a ritenere che il sistema di sicurezza e di autenticazione forte, in uso alla Banca, fosse operativo e che – in assenza di altre o diverse circostanze che possano, ad esempio, fare ritenere l'illecita captazione di dati da parte di terzi (…) – l'esecuzione di detto bonifico sia avvenuta con la collaborazione o, comunque, in conseguenza di una grave negligenza dell'utilizzatore nella custodia delle proprie credenziali*".

Nello stesso senso, l'anno successivo, la Corte di Cassazione, con sentenza 12 febbraio 2024, n. 3780 ribadiva che "*la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici (…) va esclusa se ricorre una situazione di colpa grave dell'utente configurabile, ad esempio, nel caso di protratta attesa prima di comunicare l'uso non autorizzato dello strumento di pagamento*".

Per andare esente da responsabilità, dunque, in sede di giudizio l'istituto di credito è tenuto a dare dimostrazione di aver adottato sistemi di sicurezza adeguati e che l'evento fraudolento è direttamente riconducibile ad un comportamento del cliente connotato da dolo o colpa grave. Quest'ultima prova può essere fornita anche tramite presunzioni, purché gravi, precise e concordanti.

La giurisprudenza chiarisce, inoltre, che non è sufficiente una mera disattenzione della vittima: la colpa grave richiede una condotta caratterizzata da imprudenza o negligenza inescusabili, riscontrabili in particolare quando l'utente viola gli oneri di custodia e di diligente utilizzo degli strumenti di pagamento ovvero quando ometta di comunicare tempestivamente all'intermediario il furto, lo smarrimento o l'appropriazione indebita degli stessi.

Nel panorama giurisprudenziale, il tema della colpa grave del cliente è oggetto di letture non uniformi: gli orientamenti oscillano in funzione del livello di rigore con cui il giudice valuta la condotta dell'utente, spaziando da impostazioni maggiormente garantiste — che richiedono una prova particolarmente stringente dell'imprudenza inescusabile — a interpretazioni più severe, nelle quali anche comportamenti ritenuti sintomatici di scarsa diligenza possono essere considerati idonei a integrare la colpa grave. Questa eterogeneità riflette la complessità delle dinamiche fraudolente e la necessità di calibrare l'analisi caso per caso, alla luce delle specifiche circostanze operative e delle misure di sicurezza effettivamente adottate.

In linea generale, è comunque possibile osservare che la giurisprudenza ha riconosciuto una colpa grave in capo al cliente in tutti quei casi in cui quest'ultimo abbia fattivamente e incautamente cooperato alla realizzazione della truffa. Tali ipotesi ricorrono, ad esempio, quando il cliente conservi il codice pin vicino al bancomat (Tribunale Roma, 3 gennaio 2024; Tribunale Civitavecchia, 30 giugno 2025, n. 797) ovvero quando effettui tardivamente la denuncia dell'evento fraudolento (Tribunale Bari, 13 febbraio 2025, n. 544) o, ancora, quando comunichi a terzi le credenziali ignorando il contenuto degli sms alert ricevuti dalla propria banca (Tribunale di Roma, 11 settembre 2023, n. 12832). Ancora, è stata riconosciuta una grave negligenza allorché l'utente abbia fornito a terzi ripetutamente le credenziali (Tribunale Torre Annunziata, 15 luglio 2024, n. 2083) o abbia inserito personalmente, a seguito di contatto da parte di terzi, le credenziali necessarie per l'autenticazione a due fattori (Tribunale Napoli Nord 3 gennaio 2024).

Si tratta, in definitiva, di fattispecie nelle quali il danneggiato adotta condotte connotate da una ingiustificata credulità, arrivando anche a fornire volontariamente le proprie credenziali a soggetti sconosciuti, pur essendo consapevole – come chiaramente indicato dai siti e dalle comunicazioni ufficiali degli istituti di credito – che la banca non richiede mai tali dati attraverso canali informali.

Di contro, la responsabilità del prestatore di servizi è stata riconosciuta ogni qualvolta sia emersa l'assenza di sistemi di presidi di sicurezza conformi agli standard normativi ed idonei a prevenire le truffe, come nei casi in cui la banca abbia omesso l'invio degli sms alert o di richiedere l'autenticazione a due fattori (Corte Appello Venezia, 17 marzo 2025, n. 699). Altresì, i giudici hanno imputato la responsabilità agli intermediari in caso di truffe articolate, difficili riconoscibili da parte del cliente, perché basate su sofisticate tecniche di spoofing, con sms e telefonate provenienti in apparenza proprio dalla Banca (Tribunale Milano, 21 febbraio 2025, n. 1514; Tribunale Salerno, 23 gennaio 2025, n. 348).

4. ABF: responsabilità del prestatore e colpa grave dell'utilizzatore

Anche l'Arbitro Bancario Finanziario (ABF) ha analizzato i profili di responsabilità del prestatore dei servizi di pagamento e le possibili esenzioni, tracciando, nei suoi più recenti orientamenti, confini maggiormente nitidi sulla ripartizione delle responsabilità in caso di operazioni non autorizzate.

Il principio di fondo resta quello fissato dal D.lgs. 11/2010 (attuativo delle direttive PSD e PSD2): se l'u-

vedi l'articolo online

tente non ha agito con dolo o colpa grave, la banca deve rimborsare integralmente le somme sottratte. Ma la definizione di "colpa grave" continua a essere terreno di scontro.

Phishing: consenso apparente, ma non autorizzazione

Nel caso deciso dal **Collegio ABF di Milano n. 3501/2025**, il ricorrente aveva denunciato la sottrazione di una somma dal proprio conto corrente a seguito dell'esecuzione di un bonifico fraudolento disposto verso un beneficiario sconosciuto. L'episodio era avvenuto dopo una chiamata sospetta proveniente da un numero telefonico apparentemente riconducibile all'intermediario bancario.

La banca, nel respingere la richiesta di rimborso, aveva sostenuto che l'operazione risultava "autenticata" tramite il dispositivo del cliente, dunque da considerarsi come autorizzata. Tuttavia, il Collegio ha rigettato tale impostazione, chiarendo che:

"*La mera riconducibilità tecnica dell'operazione al dispositivo dell'utente non è sufficiente a qualificarla come autorizzata*."

Dai LOG prodotti dall'intermediario era emerso che il *device* utilizzato per l'autenticazione fosse effettivamente quello intestato al cliente. Nonostante ciò, l'ABF ha sottolineato che tale circostanza non dimostra l'effettiva volontà del pagatore di eseguire il bonifico, ribadendo che il concorso causale del cliente non implica necessariamente consenso.

In particolare, il Collegio ha affermato che: "*Se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di 'consenso', dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il prestatore dei servizi di pagamento*."

Il principio richiamato fa leva sull'art. 5 del D.lgs. 11/2010, secondo cui un'operazione di pagamento può considerarsi autorizzata solo se il consenso è libero, consapevole e conforme alle modalità pattuite tra banca e cliente.

L'ABF ha poi distinto il caso in cui il truffatore predisponga l'operazione e il cliente si limiti a confermarla — ad esempio, tramite una notifica push o l'inserimento di un codice di sicurezza — in buona fede, credendo di autorizzare un'operazione lecita. In tali situazioni, osserva il Collegio: "*Laddove l'operazione di pagamento on-line sia stata preparata dal truffatore e autorizzata dal cliente tramite la ricezione della notifica push e l'inserimento della biometria o di un codice di conferma, questa non può ritenersi eseguita per intero dal pagatore, e quindi non può considerarsi sussistente il requisito necessario per escludere il regime di responsabilità previsto dalla PSD2*."

Pertanto, mancando un consenso libero e consapevole, l'operazione non può considerarsi autorizzata ai sensi della legge. Il Collegio ha così concluso che:

"*Quando il truffatore imposta l'operazione e la vittima la conferma credendo di validare un'azione legittima, manca il consenso libero e consapevole richiesto dall'art. 5 del D.lgs. 11/2010*".

In sintesi, l'ABF di Milano ha stabilito che, in casi di phishing o truffe telefoniche, la sola circostanza che il cliente abbia tecnicamente confermato l'operazione non basta a trasferire su di lui la responsabilità. L'intermediario deve quindi rimborsare integralmente l'importo sottratto, non essendo provata l'autorizzazione effettiva del pagamento.

Diverso l'esito nel **caso ABF Milano n. 1621/2025**, in cui il cliente, pur vittima di phishing, aveva materialmente inserito i dati e confermato il pagamento. Il Collegio ha preliminarmente osservato che il bonifico contestato è stato effettivamente eseguito dallo stesso cliente, che ha inserito le credenziali di accesso e completato tutte le procedure di autenticazione richieste dal sistema.

Il passaggio centrale della decisione recita:

"*La narrazione dei fatti consegnata al ricorso e alla denuncia versata in atti induce a ritenere che l'operazione contestata (un bonifico effettuato l'11 luglio 2024 alle ore 12:30 per un importo complessivo di € 4.520,00) sia stata eseguita direttamente dal cliente, il quale – cadendo vittima di un raggiro – ha personalmente disposto il pagamento, seguendo le istruzioni impartite dal frodatore*."

Alla luce di ciò, il Collegio ha richiamato un orientamento consolidato, già espresso in precedenti decisioni (Milano nn. 8007/2020; 19945/2021; 11546/2019; Roma n. 4658/2021), secondo cui: "*Quando l'o-*

perazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'operazione non può configurarsi come fraudolenta e perciò rientrante nell'ambito di applicazione della disciplina di cui al D.lgs. 27 gennaio 2010, n. 11, dovendosi la stessa considerare invece come autorizzata."

E ancora: "*Per quanto la volontà del cliente di effettuare tali operazioni sia stata viziata per effetto del raggiro subito dal terzo ignoto, l'intermediario non poteva che considerare autorizzati i pagamenti effettuati personalmente dal titolare dello strumento di pagamento, non avendo alcuna possibilità di accorgersi della truffa perpetrata ai danni del cliente*".

Il Collegio ha anche escluso eventuali profili di responsabilità dell'intermediario, osservando che la truffa non presentava caratteri di particolare sofisticazione tali da far pensare a un attacco ai canali bancari: "*È sufficiente rilevare che la truffa non presenta certo caratteri di particolare raffinatezza o insidiosità che possano far pensare alla compromissione dei canali dell'intermediario: il ricorrente riferisce – senza fornirne prova – che la chiamata proveniva da un numero (+39011*446) in alcun modo riconducibile al convenuto, come pure può dirsi per la e-mail di conferma dell'avvenuto storno dell'operazione contestata.*".

Furti lampo e custodia del PIN

Nelle decisioni **ABF Milano nn. 2518 e 2520 del 2025**, l'Arbitro ha adottato una linea rigorosa verso i clienti che subiscono furti "immediati".

In particolare, nei casi citati le operazioni fraudolente erano avvenute a pochi minuti dallo smarrimento della carta: *"La brevità del lasso temporale intercorso tra la sottrazione della carta e il primo utilizzo fraudolento rappresenta un indice significativo della colpa grave del cliente nella custodia delle credenziali dello strumento di pagamento"*. Nessun risarcimento, dunque, per l'utente.

Ancora più netta la **decisione n. 2752/2025**, sempre del Collegio di Milano secondo cui "*è noto come proprio il breve lasso temporale che intercorre tra il momento del furto e l'utilizzo della carta riveste valore presuntivo della mancata corretta conservazione delle password, il che porta a concludere che l'utente non abbia correttamente adempiuto agli obblighi di diligenza imposti dalla normativa di riferimento, dovendosi di conseguenza affermare la relativa colpa grave*". Nel caso in commento tra il furto e i prelievi erano trascorsi appena 13 minuti.

Secondo il Collegio, è altamente improbabile che un terzo possa individuare casualmente il PIN senza una precedente conoscenza, anche indiretta, del codice. L'ipotesi più plausibile è che carta e PIN fossero conservati insieme – e quindi la banca non risponde.

Sim swap: responsabilità condivisa (ma non sempre)

Il fenomeno della "SIM swap fraud" – in cui un truffatore duplica la SIM dell'utente per ricevere gli SMS di conferma – resta una zona grigia.

Tale è una tecnica di attacco che consente di avere accesso al numero di telefono del legittimo proprietario e violare determinate tipologie di servizi online che usano proprio il numero di telefono come sistema di autenticazione. Come è stato asserito dal Collegio di Roma nel maggio 2020, "*In diritto la vicenda qui considerata si inquadra nella casistica del furto di strumenti di pagamento e di identità elettronica e va pertanto valutata alla luce delle vigenti disposizioni normative in materia di servizi di pagamento, con particolare riguardo agli artt. 7, 10 e 12 del d.lgs. n. 11/2010*". Di conseguenza, *"l'intermediario che non intenda farsi carico delle perdite sofferte dal cliente per operazioni che non siano state effettivamente autorizzate, ha l'onere (i) di provare innanzitutto di aver adottato un sistema di "autenticazione forte" per l'utilizzo degli strumenti di pagamento da parte del cliente nonché, nel caso specifico, che le operazioni siano state correttamente autenticate, registrate e contabilizzate; (ii) e poi, fornita questa preliminare prova, di provare altresì, se non il dolo, almeno la colpa grave del cliente nell'aver reso possibile il compimento delle operazioni non autorizzate*". Data la sofisticata truffa, il PSP non ha modo - se in presenza di reali casi di sim swap fraud - di dimostrare la colpa grave o il dolo dell'utilizzare. Per tale motivo, la tesi maggioritaria vedeva quest'ultimo responsabile del danno cagionato all'utilizzatore, insieme all'operatore telefonico (**Collegio di Roma decisione n. 9504/2020**).

Home banking e indirizzi IP "sospetti"

Non basta che un bonifico parta da un IP diverso per invocare la responsabilità della banca. In particolare, un istituto di credito veniva accusato dal ricorrente, suo cliente, di non aver monitorato adeguatamente le operazioni del conto corrente di quest'ultimo, il che non aveva consentito di bloccare una

truffa informatica in corso. La banca ha spiegato che sarebbe impossibile monitorare gli indirizzi IP di tutti i clienti, ossia quel codice che identifica univocamente un dispositivo, e segnalarlo ogni volta che quest'ultimo cambi. Se non vi sono precise prove di forzatura di accesso al conto del cliente, non c'è necessità di allertarsi se un pagamento viene fatto da un dispositivo diverso. Ad oggi, tutti hanno in possesso almeno due dispositivi elettronici con cui effettuare un pagamento. Nella ricostruzione della decisione dell'ABF in analisi, si legge che *"gli indirizzi IP riconducibili all'operatività disconosciuta e quelli invece riferiti all'operatività della cliente, di per sé sola non può essere intesa quale segnale che debba automaticamente allertare i sistemi bancari poiché altrimenti, vista l'operatività odierna degli utenti, la stessa operatività bancaria sarebbe soggetta a continui blocchi: in altri termini, paralizzata."* Nel caso di specie, il ricorso è stato respinto e dunque si è data ragione alla banca. Essa, difatti, *"ha dimostrato, mediante le schermate prodotte in atti, che le operazioni risultano autorizzate con inserimento sia delle credenziali di accesso statiche, sia di quelle dinamiche, conformemente alla disciplina dei sistemi di autenticazione forte"* (**Collegio di Torino decisione n. 5133/2022**).

Truffe da marketplace e bonifici "volontari"

C'è poi la frontiera più recente: i raggiri su piattaforme di compravendita, dove le vittime vengono indotte a disporre bonifici verso falsi venditori.

Nei casi **ABF Milano n. 1627/2025** e **Torino n. 1801/2025**, l'Arbitro ha escluso la responsabilità delle banche poiché le operazioni erano state disposte personalmente dai clienti.

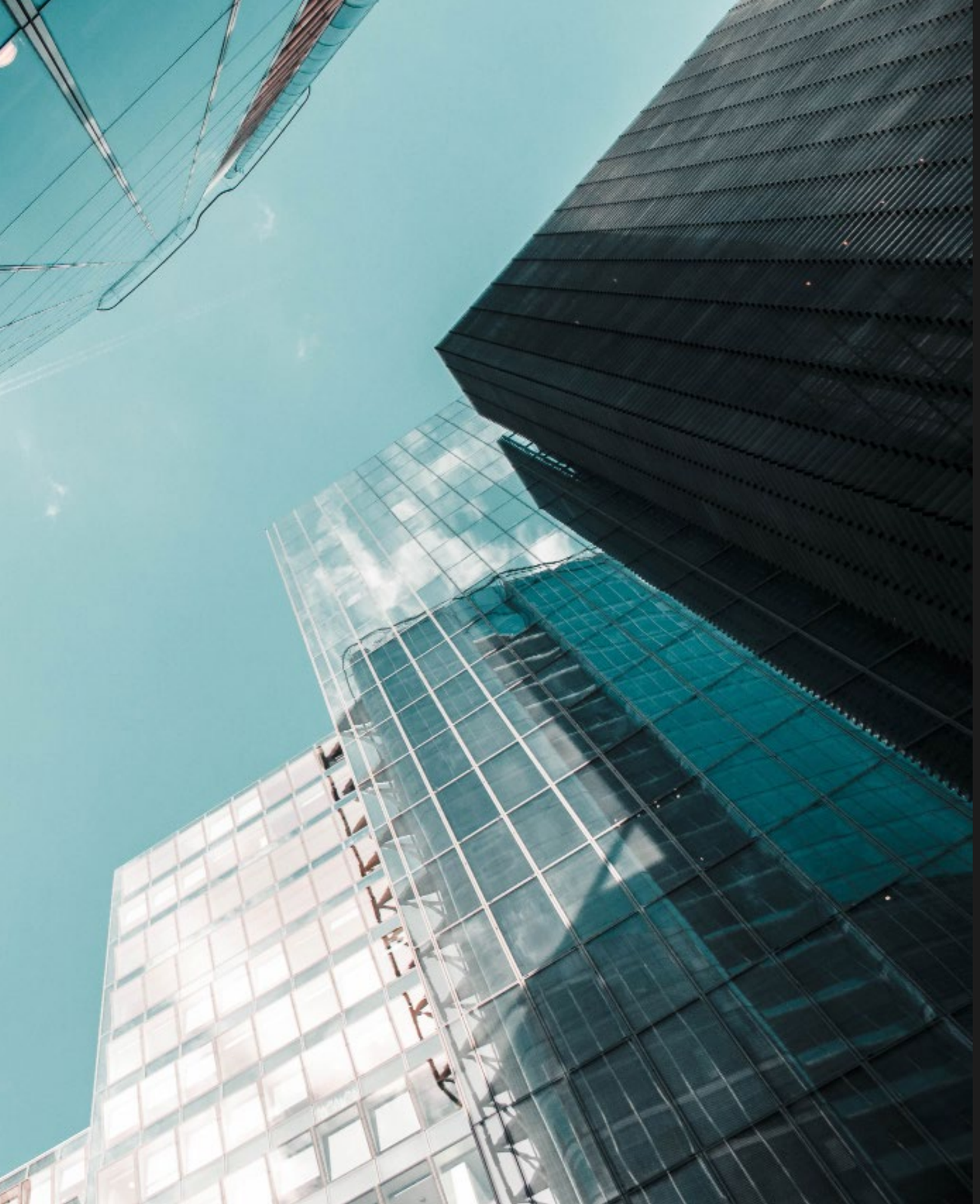
In particolare, in entrambe le decisioni si fa riferimento all'art. 24 del D.lgs. 11/2010 secondo cui la banca non è tenuta a verificare la corrispondenza tra nominativo del beneficiario e IBAN: l'errore, se indotto, resta a carico dell'utente.

Dalle ultime pronunce emerge una tendenza chiara: l'ABF protegge l'utente, ma solo se dimostra un comportamento diligente. Chi comunica codici via telefono, conserva PIN insieme alla carta o denuncia il furto con ritardo rischia di perdere il diritto al rimborso.

In altri termini la colpa grave dell'utilizzatore è l'unico varco che consente all'intermediario di sottrarsi alla responsabilità. Un equilibrio sottile, destinato a essere continuamente ridefinito, man mano che le frodi digitali si evolvono più rapidamente delle stesse norme di sicurezza.

5. Conclusioni

In conclusione, il fenomeno delle frodi informatiche continua a evolversi con rapidità, assumendo forme sempre più sofisticate e difficilmente prevedibili anche da parte degli operatori più attenti. Tale dinamicità si riflette inevitabilmente sul piano interpretativo: l'elaborazione giurisprudenziale e le decisioni dell'Arbitro Bancario Finanziario presentano, ad oggi, orientamenti non uniformi, oscillanti tra la tutela dell'utente e la valorizzazione del principio di diligenza dell'intermediario. In un contesto in costante trasformazione, saranno quindi determinanti l'evoluzione legislativa e tecnologica, al fine di definire un quadro più chiaro e coerente, capace di garantire un equilibrato bilanciamento tra la protezione dei clienti e la sostenibilità operativa del sistema bancario.



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it