ANDREA GENOVESE

L'UTILIZZO FRAUDOLENTO DEGLI STRUMENTI DI PAGAMENTO

Lefebvre Giuffrè

Isbn 9788828867487

Estratto dal volume:

I TRATTATI GIUFFRÈ

DIRITTO BANCARIO

diretto da
Fernando Greco - Gianfranco Liace

II. INFORMAZIONE, TRASPARENZA E TUTELA

2025

Capitolo 17

L'UTILIZZO FRAUDOLENTO DEGLI STRUMENTI DI PAGAMENTO

di *Andrea Genovese*

Sommario: 1. Introduzione. — 2. La disciplina di speciale protezione per l'utente in caso di disconoscimento di un'operazione di pagamento. Artt. 10 e 11, d.lgs. 27 gennaio 2010, n. 11. — 3. Il disconoscimento dell'operazione di pagamento. — 4. La responsabilità del titolare dello strumento di pagamento. — 5. Eventuale concorso di colpa dell'intermediario nella causazione del danno patito dall'utente: *a*) il servizio di notifica « *sms-alert* ». — 6. *Segue*: *b*) gli indici di anomalia dell'operazione di pagamento. — 7. Il caso della « SIM *swap fraud* » e la posizione della giurisprudenza. — 8. La spedizione della carta di pagamento. La tecnica del c.d. *boxing*.

Riferimenti normativi: artt. 1176, 1218, 1226, 1227 c.c.; d.lgs. 27 gennaio 2010, n. 11.

Riferimenti giurisprudenziali: Cass., sez. I, 13 marzo 2023, n. 7214; Cass., sez. VI, 26 novembre 2020, n. 26916; ABF, Collegio di Coordinamento, decisione 10 ottobre 2019, n. 22745; ABF, Collegio di Roma, decisione 5 aprile 2013, n. 1820; ABF, Collegio di Coordinamento, decisione 26 ottobre 2012, n. 3498.

Bibliografia: F. Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione della responsabilità. Dagli orientamenti attuali alla revisione della PSD*, in *Dir. banc. merc. fin.*, 2017, 150 ss.; S. Cirelli, *Utilizzo non autorizzato dello strumento di pagamento e responsabilità della banca*, in *Giur. comm.*, 2022, 438 ss.; R. Frau, Home banking, *captazione di codici di accesso ed esclusione della responsabilità della banca*, in *Resp. civ. prev.*, 2024, 163; G. Liace, F. Fiorucci, *Conto corrente. Contratti bancari*, in *Commentario del Codice Civile e codici collegati Scialoja-Branca-Galgano*, a cura di G. De Nova, Bologna, Zanichelli, 2025; G. Liberati Buccianti, *Carte di pagamento e (in)debiti utilizzi nelle decisioni dell'Arbitro Bancario Finanziario*, in *I contratti bancari*, a cura di C. M. Bianca, Roma, Dike, 2013; F. Marasà, *Utilizzo fraudolento di carta bancomat e diligenza professionale della banca*, in *Banca borsa tit. cred.*, 2016, 396 ss.; S. Martinelli, *Sicurezza informatica degli istituti di credito e responsabilità contrattuale*, in *Giur. it.*, 2017, c. 2069 ss.; L. Muttini, *Frodi informatiche e responsabilità della banca: i nuovi orientamenti dell'arbitro bancario finanziario*, in *Riv. dir. banc.*, 2021, 41; M. Semeraro, *Modelli di responsabilità e private enforcement: appunti su PSD2 e operazioni di pagamento non autorizzate*, in *Riv. dir. banc.*, 2022, 825.

1. Introduzione.

È sempre più frequente la consumazione di frodi informatiche con le quali i malfattori riescono a carpire i dati dei clienti delle banche al fine dell'esecuzione di operazioni di pagamento non autorizzate, attraverso l'esecuzione di bonifici bancari o l'uso di carte di debito o di credito (1). Tra le principali frodi legate all'utilizzo degli strumenti di pagamento, come tali menzionate nell'ultima **Relazione sull'attività dell'Arbitro Bancario Finanziario** del giugno 2024 (2), si possono certamente rammentare:

> « *i*) quella conosciuta con la denominazione « *man in the browser* », che si perfeziona mediante un software malevolo (malware) che si interpone tra il computer della vittima e il sistema della banca.
> *ii*) Poi si ha la frode dello *skimming*, che consiste in una tecnica attraverso la quale, grazie all'utilizzo di uno *skimmer*, ossia di uno strumento che permette di leggere e memorizzare il contenuto presente sulla banda magnetica di una carta elettronica con cui entra in contatto, il malfattore ne consegue il possesso dei dati, come il codice pin (3), attraverso i quali riesce a compiere l'operazione fraudolenta. In via descrittiva, può quindi dirsi che con lo *skimming* avviene una sorta di « clonazione » delle carte di credito e di debito.
> *iii*) Ma il principale illecito — sia per l'alta frequenza con cui avviene consumato, sia per gli ingenti volumi delle operazioni non autorizzate che allo stesso si accompagnano — è rappresentato dal *phishing*. Esso consiste in una tecnica fraudolenta mediante la quale, grazie all'invio di un c.d. « messaggio civetta » apparentemente riconducibile alla banca o ad altra impresa affidabile (ad es., di trasporti, di commercio elettronico), il malfattore, con la cooperazione colposa dell'utente, riesce ad entrare in possesso degli elementi identificativi dello strumento di pagamento, come il nome utente, la password, il codice otp (4), il pin, ecc., con cui riesce ad eseguire illegittime transazioni *online* ».

In argomento, la giurisprudenza dell'ABF, in particolare del Collegio di Coordinamento, è solita distinguere:

---

(1) Trib. Rovigo, 10 luglio 2023, n. 603. In dottrina, si v. F. Liace, F. Fiorucci, *Conto corrente. Contratti bancari*, in *Commentario Scialoja-Branca-Galgano*, a cura di G. De Nova, Bologna, Zanichelli, 2025, 396.

(2) La Relazione è consultabile all'indirizzo *arbitrobancariofinanziario.it*.

(3) « Pin » è l'acronimo di « *personal identification number* », cioè numero di identificazione personale.

(4) « Otp » è l'acronimo di « *one-time password* », ossia una password valida solo per una singola sessione di accesso.

« *i*) le ipotesi di *phishing* tradizionale nelle quali il messaggio civetta consiste in una semplice e-mail, telefonata (c.d. *vishing*) (5) o *sms* (c.d. *smishing*) (6), attraverso i quali il cliente della banca è invitato e persuaso a rilevare le credenziali di accesso al proprio strumento di pagamento, ad es. mediante digitazione delle stesse su di una pagina web molto simile a quella della banca (c.d. pagina clone). In questo tipo di frodi che muovono dall'invio della mail o dell'*sms*, l'utente della banca riceve di regola anche una successiva telefonata da parte di un sedicente operatore bancario, o apparente alle forze dell'ordine (7), con cui viene convinto a comunicare i dati necessari all'esecuzione di questa o quella transazione online.
ii) Si ha poi una forma più insidiosa di *phishing*, definita *spoofing*, che avviene attraverso un metodo di intrusione caratterizzato da un particolare « effetto sorpresa », capace di spiazzare anche l'utilizzatore mediamente diligente, grazie alla perfetta inserzione della mail o dell'*sms* civetta nell'ambiente informatico originale e nella correlata simulazione di un messaggio che potrebbe apparire genuino. In questi casi, l'attacco informatico impiega, in vario modo, la falsificazione dell'identità (*spoof*) ad es. di un *host* all'interno di una rete o del mittente di un messaggio o di una telefonata » (8) (Collegio di Coordinamento dec. 26 ottobre 2012, n. 3498 e Collegio di Roma, dec., 5 aprile 2013, n. 1820).

---

(5) Il « *vishing* », noto anche come « *phishing* vocale », è una truffa in crescente diffusione che sfrutta le chiamate telefoniche per ottenere informazioni personali, in particolare dati bancari e relativi alle carte di credito, con l'obiettivo di sottrarre somme di denaro di varia entità. Generalmente, i malfattori si spacciano per operatori di istituti bancari o società che gestiscono *bancomat* e carte di pagamento. Contattano le vittime segnalando presunte anomalie nei loro conti o transazioni e le convincono, con tono rassicurante, ad eseguire false procedure di sicurezza, che in realtà servono solo a carpire informazioni sensibili.

(6) Lo « *smishing* », o « *phishing* tramite *sms* », è una tecnica di frode che sfrutta i messaggi di testo e i sistemi di messaggistica, inclusi quelli delle piattaforme social, per ottenere dati personali con finalità fraudolente, spesso finalizzate alla sottrazione di denaro da conti bancari e carte di credito.

Questi messaggi ingannevoli spingono le vittime ad agire con urgenza, inducendole a cliccare su link sospetti o a fornire informazioni sensibili per evitare presunti problemi, come un'operazione fraudolenta che si sta consumando all'estero, il blocco di un conto, di una carta di credito o altre conseguenze negative.

Il truffatore, il c.d. *smisher*, invia messaggi con richieste fraudolente, tra cui: *a*) cliccare su un link che rimanda a un modulo *online* per inserire dati personali, bancari o della carta di credito. Talvolta, il link può installare *malware* sul dispositivo, consentendo ai criminali di rubare informazioni archiviate o persino di accedere alle app di *home banking* e pagamento; *b*) scaricare un allegato che contiene *software* malevolo capace di compromettere il controllo dello smartphone o di accedere ai dati memorizzati; *c*) rispondere al messaggio fornendo dati sensibili, come codice fiscale, pin della carta di debito, credenziali per l'*Internet banking*, numero e codice di sicurezza della carta di credito o password temporanee otp per le operazioni finanziarie; *d*) chiamare un numero di telefono, dove un sedicente operatore o un sistema automatizzato richiede informazioni personali e bancarie con l'intento di sottrarre fondi o compromettere i conti della vittima.

(7) Ad. es., il sedicente comandante dei carabinieri, si v. ABF, Collegio di Torino, dec. 21 novembre 2024, n. 12063.

(8) Il « CLI Spoofing », acronimo di *Calling Line Identification Spoofing*, è una tecnica ingannevole che permette di manipolare il numero di telefono visualizzato dal destinatario di

Alla crescita di questi fenomeni si è accompagnata l'esecuzione di intense campagne di informazione e sensibilizzazione, attraverso le quali i clienti delle banche sono stati resi edotti sul fatto che, ad es., mai un operatore bancario richiederà loro di comunicargli i dati personali e/o identificativi, piuttosto che le credenziali riservate di accesso allo strumento di pagamento (9).

Ciononostante, può residuare una qualche forma di responsabilità in capo alla banca derivante o da discipline recanti una speciale forma protezione a favore dell'utente, o dall'applicazione di principi generali dell'ordinamento. A questo ultimo riguardo, ad es., la giurisprudenza ha rammentato che nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza del debitore deve valutarsi con riguardo alla natura dell'attività esercitata *ex* art. 1176, comma 2, c.c. In particolare, nel rapporto contrattuale di *home banking*, agendo quale contraente qualificato, la banca — ormai a conoscenza delle modalità sempre più sofisticate delle frodi telematiche — deve dirsi tenuta a prestare la massima attenzione, anche aggiornando e migliorando i sistemi di sicurezza, al fine di renderli sempre più capaci di intercettare e bloccare eventuali operazioni sospette (10).

2. La disciplina di speciale protezione per l'utente in caso di disconoscimento di un'operazione di pagamento. Artt. 10 e 11, d.lgs. 27 gennaio 2010, n. 11.

In presenza del disconoscimento di un'operazione di pagamento da parte dell'utente, grava sulla banca l'onere di dimostrare che la stessa è stata correttamente autenticata, registrata e contabilizzata. È quindi sufficiente che la banca non assolva al detto onere della prova, affinché sorga il diritto del cliente ad ottenere il rimborso dell'operazione contestata in conformità a quanto previsto dagli artt. 10 e 11, d.lgs. 27 gennaio 2010, n. 11, come modificati dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della Dir. (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2),

---

una chiamata. Questo metodo è sovente utilizzato da malfattori per far apparire il proprio numero come appartenente a un'organizzazione affidabile, come una banca, un'azienda, un ente pubblico o persino un contatto noto, al fine di guadagnare la fiducia della vittima.

(9) Nella « Relazione sull'attività dell'Arbitro Bancario Finanziario » relativa al 2023 (si v., nt. 2), si richiama la campagna di informazione « I Navigati - Informati e Sicuri », realizzata per favorire l'uso sicuro e consapevole dei canali e degli strumenti digitali e sensibilizzare i clienti sui rischi di attacchi e frodi online nella fruizione di servizi finanziari, consultabile anche all'indirizzo *bancaditalia.it.*

(10) Trib. Milano, 4 dicembre 2014; S. MARTINELLI, *Sicurezza informatica degli istituti di credito e responsabilità contrattuale*, in *Giur. it*., 2017, c. 2069 ss.

che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il Reg. (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015, relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta (11).

In particolare, in base all'art. 10, comma 1, d.lgs. 27 gennaio 2010, n. 11, in caso di contestazione di un'operazione di pagamento da parte dell'utente, grava sul prestatore del servizio di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha risentito delle conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri malfunzionamenti (12).

È quindi sufficiente che l'utente esegua il disconoscimento di un'operazione fraudolenta affinché si determini questa significativa inversione dell'ordinario assetto dell'onere della prova regolato dall'art. 2697 c.c. Il disconoscimento dell'operazione di pagamento ribalta sul prestatore del servizio di

---

(11) Il Collegio di coordinamento ABF, in più occasioni, ha precisato che la disciplina in esame istituisce « un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento » (ABF, Collegio di Coordinamento, dec. 24 giugno 2014, n. 3947).

(12) La giurisprudenza di merito ha sottolineato che in tema di responsabilità della banca per operazioni in conto corrente effettuate a mezzo di strumenti elettronici, nel caso in cui il correntista neghi di aver autorizzato l'operazione di pagamento, è onere dell'intermediario dimostrare sia l'insussistenza di malfunzionamenti nel sistema, sia l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni disconosciute; è altresì onere dell'intermediario dimostrare ogni altro fatto idoneo ad integrare la colpa grave dell'utilizzatore. In mancanza, la banca sopporta integralmente le conseguenze delle operazioni disconosciute, senza alcuna limitazione o franchigia. In tal senso si veda Trib. Biella, 10 luglio 2024, n. 190. In dottrina si vedano F. Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione della responsabilità. Dagli orientamenti attuali alla revisione della PSD*, in *Dir. banc. merc. fin.*, 2017, 150 ss.; S. Cirelli, *Utilizzo non autorizzato dello strumento di pagamento e responsabilità della banca*, in *Giur. comm.*, 2022, 438 ss.

pagamento l'onere della prova dell'autenticazione forte della stessa operazione (c.d. *strong customer authentication*) (13). Si tratta, in particolare, di una procedura che permette di convalidare l'identificazione dell'utente mediante l'uso di due o più elementi di autenticazione (c.d. « autenticazione a due fattori »), appartenenti ad almeno due categorie tra le seguenti:

i) elemento della conoscenza (un qualcosa che solo l'utente conosce, come, ad es., una password o un pin). L'*European Banking Authority* (14) con la *Opinion* del 21 giugno 2019 ha peraltro ritenuto che i dettagli stampati sulla carta di pagamento non costituiscano un elemento di possesso e nemmeno un elemento di conoscenza ai fini della SCA;

ii) elemento del possesso (qualcosa che solo l'utente possiede, come un token/chiavetta, o uno smartphone);

iii) elemento dell'inerenza (una cosa che caratterizza l'utente, come il riconoscimento facciale o l'impronta digitale).

La mancata osservanza dell'onere della prova in rassegna conduce quindi alla costituzione del diritto a favore dell'utente di ottenere il rimborso dell'importo dall'operazione di pagamento fraudolenta, indipendentemente dal grado di colpa nel quale quest'ultimo sia in ipotesi incorso; il tutto, verrebbe da dire, in applicazione di una sorta di responsabilità oggettiva per l'accaduto.

Nella prassi che registra ciò che normalmente accade nelle aule delle corti o in occasione delle procedure arbitrali presso l'ABF, la banca è solita cercare di provare l'autenticazione forte dell'operazione contestata mediante la produzione in atti delle tracciature informatiche della stessa (ad es. con i dati dei relativi log), una volta rese leggibili e trasparenti mediante la produzione in atti di un'idonea legenda.

Per quanto concerne il possibile riutilizzo di questi fattori di autenticazione in caso di più operazioni compiute all'interno di un'unica sessione *online*, l'EBA si è favorevolmente pronunciata, con la Q&A 2018/4141, appunto nel senso della possibilità di riutilizzare un fattore di autenticazione

---

(13) Il concetto « autenticazione forte », o « *strong customer authentication* », con l'acronimo di SCA, trova la propria definizione all'art. 1, comma 1, lett. *q-bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): « 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 ».

(14) Autorità Bancaria Europea, spesso citata con l'acronimo di EBA.

di un'operazione nell'ambito della medesima sessione (15). Detto altrimenti, è reputata conforme al quadro normativo sopra delineato l'esecuzione di un'operazione di pagamento mediante inserimento di un solo fattore di autenticazione, tutte le volte in cui si procede al riutilizzo di un secondo fattore di diversa natura già inserito nella stessa sessione per l'accesso al conto, in presenza del *dynamic linking* (16).

3. Il disconoscimento dell'operazione di pagamento.

Nella prassi, il disconoscimento dell'operazione fraudolenta è solito avvenire attraverso la compilazione, da parte del cliente, di un modulo standard messogli a disposizione dalla banca, e al quale va di regola allegata la copia della denuncia dell'illecito all'autorità giudiziaria o di pubblica sicurezza.

Si deve porre in rilievo che l'art. 10, comma 1, d.lgs. 27 gennaio 2010, n. 11, non può trovare applicazione tutte le volte in cui l'operazione di pagamento non possa dirsi disconosciuta, e ciò si verifica quando la stessa operazione sia stata eseguita direttamente dall'utente. Se eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'operazione si considera infatti autorizzata e quindi non soggetta alla rammentata disciplina di particolare favore per il cliente.

Ciò posto, si fa presente che i Collegi ABF sono soliti distinguere tra:

i) operazioni autorizzate con l'intervento parziale del pagatore (ad es., quando il pagatore autorizza l'operazione precedentemente inserita dal frodatore);

ii) e operazioni eseguite per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione).

In particolare, secondo l'orientamento condiviso dei Collegi ABF, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è solo

---

(15) ABF, Collegio di Bologna, dec. 23 novembre 2021, n. 23858. Si v., altresì, ABF, Collegio di Torino, dec. 25 settembre 2024, n. 10061, nella quale si legge: « proprio la citata decisione del Collegio di Napoli, 7 marzo 2022, n. 4003, ha precisato che l'European Banking Authority (EBA) si è favorevolmente pronunciata, con la Q&A 2018/4141, in ordine alla possibilità di riutilizzare un fattore di autenticazione, affermando che "quando si avvia un pagamento, la SCA può quindi dirsi realizzata quando uno degli elementi utilizzati nel momento in cui il cliente ha avuto accesso al proprio conto di pagamento online (anche tramite un'app mobile) viene riutilizzato in conformità con l'articolo 4 e viene richiesto l'altro elemento della SCA al momento in cui viene avviato il pagamento, a condizione che l'elemento di collegamento dinamico richiesto dall'articolo 97, paragrafo 2, PSD2 e descritto in dettaglio all'articolo 5 del regolamento delegato sia presente e collegato a quest'ultimo elemento" ».

(16) Così, ABF, Collegio di Milano, dec. 7 agosto 2024, n. 9369.

parziale (ad es., mediante inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale, prescindendo dalla nozione civilistica di « consenso », dispone che lo stesso va prestato nella forma convenuta tra il pagatore stesso ed il prestatore del servizio di pagamento (c.d. *Payment Service Provider*) (17).

Rientrano nella fattispecie delle operazioni eseguite per intero del pagatore, quelle nelle quali quest'ultimo, seguendo alla lettera le indicazioni impartite del malfattore, esegue senza consapevolezza una disposizione di pagamento. Ciò accade, ad es., nelle operazioni « sotto dettatura » (18) o nelle frodi compiute in esecuzione della tecnica nota come « *social hacking* », che consiste nell'indurre l'utente a compiere un trasferimento di somme in favore del malfattore (19).

In questi casi, infatti, l'operazione non può dirsi disconosciuta ai sensi dell'art. 5, d.lgs. 27 gennaio 2010, n. 11, perché il ricorrente è consapevole di eseguirla, anche se in ciò indotto in modo fraudolento.

Da altra angolazione, si tratta di valutare in quale fattispecie rientra il caso in cui l'utente dichiari di disconoscere l'operazione perché fraudolenta, senza tuttavia allegare e provare le circostanze di tempo e di luogo nelle quali si sarebbe consumato l'illecito utilizzo dello strumento di pagamento.

In questi casi, muovendo da una lettura essenzialmente formale delle norme di riferimento, si potrebbe raggiungere la conclusione che è sufficiente il disconoscimento dell'operazione per far gravare sull'intermediario l'onere di cui all'art. 10, comma 1, d.lgs. 27 gennaio 2010, n. 11, ossia di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata, e che la stessa non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri malfunzionamenti. Aderendo a questa ipotesi interpretativa, la ricostruzione laconica e generica della frode potrebbe essere valorizzata solo per ravvisare l'elemento della colpa grave dell'utente, ma in quanto l'intermediario abbia dato la previa prova che l'operazione di pagamento è stata oggetto di autenticazione forte da parte del cliente (20).

Una simile conclusione potrebbe tuttavia essere sottoposta a rilievo critico, anche perché capace di incentivare condotte non ossequiose dei dettami della correttezza e della buona fede da parte dell'utente, che per tale

---

(17) *Ex plurimis*, quasi testualmente, si v. ABF Collegio di Bologna, dec. 15 luglio 2014, n. 8169; ABF Collegio di Palermo, dec. 5 novembre 2024, n. 11580; ABF Collegio di Milano, dec. 10 ottobre 2024, n. 10639.

(18) ABF, Collegio di Bologna, dec. 10 luglio 2024, n. 8011; ABF, Collegio di Roma, dec. 2 ottobre 2024, n. 10302.

(19) ABF, Collegio di Bologna, dec. 6 dicembre 2024, n. 12617.

(20) ABF, Collegio di Bologna, dec. 21 aprile 2023, n. 3888.

via si vedrebbe di fatto sollevato dall'onere di specificare e di provare le circostanze che hanno fatto da sfondo alla frode, e che a ben vedere sono costitutive del diritto azionato. Le stesse circostanze dovrebbero per di più essere opportunamente segnalate anche in sede di denuncia all'autorità giudiziaria o di pubblica sicurezza. Ed è per quanto visto che, quando la narrazione della frode dovesse risultare del tutto laconica e generica, o dovesse risultare la mancata presentazione della denuncia all'autorità giudiziaria o di pubblica sicurezza, ecco allora che potrebbe dirsi integrato il « fatto noto » dal quale risalire, secondo le massime di esperienza, al « fatto più probabile che non » che l'operazione di pagamento è stata eseguita direttamente dal cliente della banca o da suo delegato, anche se indotto da terzo con dolo, con conseguente inapplicabilità della disciplina di speciale protezione di cui all'art. 10, d.lgs. 27 gennaio 2010, n. 11 [21].

4. La responsabilità del titolare dello strumento di pagamento.

L'assolvimento dell'onere della prova che l'operazione bancaria disconosciuta sia stata correttamente autentica, registrata e contabilizzata non solleva di per sé la banca dall'obbligo di indennizzare il cliente per la perdita subita.

Il Collegio di Coordinamento, con la **decisione 10 ottobre 2019, n. 22745**, ha posto in rilievo che

> « la previsione di cui all'art. 10, comma 2, del d.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano

---

[21] Sembra propendere in questa direzione l'ABF, Collegio di Roma, dec. 16 maggio 2024, n. 5990, nella quale si legge che il « Collegio di Coordinamento ha avuto modo di precisare in passato che, nel caso in cui l'istante ponga a fondamento della domanda di rimborso l'asserita 'clonazione' della carta di pagamento, egli sia comunque tenuto a provare le circostanze sulla base delle quali possa ritenersi almeno plausibile la sussistenza di un caso di clonazione. 9. Nella vicenda in esame, il ricorrente — il quale dichiara che la carta è sempre rimasta in suo possesso — non ha fornito una ricostruzione (anche minima) della dinamica della truffa subita. Per di più egli non ha presentato una denuncia in relazione alla frode asseritamente subita, circostanza che i Collegi territoriali dell'ABF ritengono rilevante come ostacolo alla ricostruzione dei fatti (cfr., per esempio, Collegio di Roma, decisione n. 9670/2023). Alla luce di quanto sopra rilevato, deve pertanto ritenersi che, in assenza dell'allegazione da parte della ricorrente di circostanze idonee a fondare e a ritenere attendibile una diversa ipotesi ricostruttiva, le operazioni di pagamento contestate siano imputabili (direttamente o, quantomeno, in ragione di una condotta gravemente colposa) al titolare dello strumento di pagamento (cfr. Collegio di Roma, decisione. n. 10723/2019, e decisione, n. 7349/2021) ».

le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente » (22).

Non essendo la dimostrazione della corretta autenticazione, contabilizzazione e registrazione dell'operazione di pagamento di per sé sufficiente a certificare che la stessa operazione è stata autorizzata dall'utente, ecco che l'art. 10, comma 2, del d.lgs. 27 gennaio 2010, n. 11, sottolinea che comunque grava sul prestatore di servizi di pagamento l'onere di provare la frode, il dolo o la colpa grave dello stesso utente nell'adempimento dei propri obblighi.

Il cliente della banca è infatti tenuto a utilizzare lo strumento di pagamento in conformità alle pattuizioni esplicitate nel contratto quadro, che ne regolano l'emissione e l'uso, oltreché a prestare la necessaria attenzione e diligenza durante l'utilizzo dello stesso strumento di pagamento. Da questa prospettiva, l'utente è quindi ad es. tenuto: *a*) a custodire con cura le credenziali e le password di accesso allo strumento di pagamento e a non comunicarle ad alcuno; *b*) a segnalare senza indugio al prestatore di servizi di pagamento, o al soggetto da questo indicato, il fatto dello smarrimento, del furto, dell'appropriazione indebita o dell'uso non autorizzato dello strumento di pagamento non appena ne venga a conoscenza.

Posto che — come anticipato — il prestatore dei servizi di pagamento che intende invocare una responsabilità esclusiva dell'utente deve fornire la prova del dolo o della colpa grave dell'utente, nella prassi accade frequentemente che l'intermediario bancario riesca a sottrarsi alla responsabilità dimostrando che il comportamento del cliente deve dirsi connotato da **colpa grave** avuto riguardo alle concrete modalità, più o meno sofisticate, attraverso le quali si è consumata la frode.

In argomento, nel caso di *phishing* tradizionale, la cooperazione colposa dell'utente ai fini della consumazione della frode appare di regola difficilmente scusabile, trattandosi ormai di un fenomeno ampiamente diffuso e noto a qualunque utente dotato di media avvedutezza e prudenza, come si reputa sia quello avvezzo all'utilizzazione dei servizi di *home banking*.

Pertanto, nell'ipotesi del *phishing* tradizionale, il cliente è normalmente giudicato vittima di colpevole credulità, in quanto portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario (23). Per questo motivo, la giurisprudenza ha potuto

(22) Si v., ad es., ABF Collegio di Bologna, dec. 4 settembre 2024, n. 9593.

(23) Trib. Palermo, 11 aprile 2024; ABF, Collegio di Bologna, dec. 29 novembre 2021, n. 24208. Si configura la colpa grave del correntista il quale, violando quel minimo grado di diligenza riconoscibile da chiunque, immette codici riservati nella pagina *web* richiamata

accertare la responsabilità del titolare dello strumento di pagamento tutte le volte in cui digiti i propri codici personali (richiestigli con una mail truffaldina), così consentendo all'ignoto malfattore di utilizzarli successivamente per effettuare un bonifico fraudolento (24).

L'ABF è invece solito ritenere sussistente la responsabilità dell'intermediario, o meglio la mancanza di colpa grave in capo all'utente, in presenza dello *spoofing*, che — come sopra visto — rappresenta una forma di aggressione informatica più insidiosa, che consiste nell'alterazione dei dati relativi al mittente di una mail o di un *sms* per far sì che essi appaiano provenire da un soggetto affidabile, ad es. attraverso la sostituzione del numero originario con un testo alfanumerico riconducibile a quello utilizzato dall'intermediario per i propri messaggi genuini. In questi casi, il cliente riceve un « messaggio civetta » che si inserisce nello storico delle comunicazioni genuine con l'intermediario, nella stessa *chat* (25).

È importante, tuttavia, porre in rilievo che l'ABF, in modo largamente condivisibile, anche in questi casi, ha ritenuto sussistere la colpa grave del cliente tutte le volte in cui, nonostante il messaggio civetta si inserisca nello storico delle conversazioni genuine con l'intermediario, rechi tuttavia indici di inattendibilità o di anomalia (ad es., l'invito a cliccare su un *link* non riconducibile all'intermediario, o la presenza di errori grammaticali o di sintassi) che avrebbero dovuto allertare l'utente mediamente avveduto (26).

Ma anche il fatto della mancata prova del messaggio civetta che l'utente assume di aver ricevuto, ovvero della telefonata che si allega essere pervenuta da parte del sedicente operatore del prestatore di servizi di pagamento (ad es., mediante allegazione dei relativi *screenshot*), permette di formulare un giudizio in termini di colpa grave, atteso che la carenza probatoria non consente di verificare se il mittente risulti effettivamente riconducibile al prestatore di servizi di pagamento, o se il cliente abbia potuto riporre un legittimo affidamento in ordine alla genuinità del messaggio o contatto telefonico (27).

---

dall'*e-mail* di *phishing*. In tal senso si veda Trib. Roma, 9 aprile 2023; Giudice di pace Roma, 6 luglio 2022, n. 13050. In dottrina si veda M. SEMERARO, *Modelli di responsabilità e private enforcement: appunti su PSD2 e operazioni di pagamento non autorizzate*, in *Riv. dir. banc.* 2022, 825.

(24) Cass., sez. I, 13 marzo 2023, n. 7214.

(25) ABF, Collegio di Milano, dec. 25 giugno 2021, n. 15621; ABF, Collegio di Torino, dec. 25 marzo 2020, n. 5647.

(26) ABF, Collegio di Bologna, decisioni 12 aprile 2024, n. 4459 e 10 maggio 2023, n. 4485; ABF, Collegio di Roma, dec. 14 febbraio 2022, n. 2695; ABF, Collegio di Milano, dec. 9 febbraio 2022, n. 2403.

(27) ABF, Collegio di Bologna, dec. 12 aprile 2024, n. 4459, cit.; ABF, Collegio di Milano, dec. 1° febbraio 2024, n. 1447.

Ancora, l'ABF è solito riconoscere l'elemento della colpa grave dell'utilizzatore non solo quando — come sopra visto — sia estremamente generica ed apodittica la narrazione dei fatti relativi alla frode, ma anche in caso di furto della borsa nella quale sia custodito lo strumento di pagamento lasciata all'interno dell'autovettura posteggiata, anche se chiusa a chiave (28). Deve dirsi infatti gravemente negligente la decisione del titolare dello strumento di pagamento di lasciare la borsa o il portafoglio all'interno della vettura parcheggiata in un luogo pubblico o aperto al pubblico.

In questi casi, inoltre, la brevità del lasso temporale che intercorre tra il momento del furto e quello del successivo prelievo con la carta sottratta, lasciano presumere che il codice pin fosse conservato congiuntamente alla stessa, e che, pertanto, l'autore del furto si sia impossessato di entrambi, con la colposa cooperazione dell'utente (29).

Non sempre la conservazione del pin congiuntamente allo strumento di pagamento è però indice di colpa grave dell'utente. Fa, infatti, eccezione a quanto appena illustrato, il caso in cui lo strumento di pagamento e le relative credenziali di accesso siano sottratti in occasione di un « furto con destrezza ». Ad avviso dei collegi ABF, si verifica questa ipotesi quando il furto dello strumento di pagamento e delle relative credenziali, che è il presupposto della successiva frode, si consuma quando il malfattore riesce a far scendere l'utente dall'autovettura con lo stratagemma, ad es., della foratura dello pneumatico o della caduta in terra delle chiavi o delle banconote (30).

5. Eventuale concorso di colpa dell'intermediario nella causazione del danno patito dall'utente: *a*) il servizio di notifica « *sms-alert* ».

Anche quando abbia assolto all'onere di provare non solo che l'operazione di pagamento disconosciuta è stata correttamente autenticata, registrata e contabilizzata, ma che il cliente ha anche serbato una condotta certamente innervata da colpa grave, può residuare un qualche margine di corresponsabilità a carico del prestatore dei servizi di pagamento.

Questo perché — in linea di massima — in presenza di operazioni di pagamento tramite servizio di *home banking*, spetta comunque all'intermediario l'onere di verificare la riconducibilità delle stesse alla volontà del

---

(28) ABF, Collegio di Bologna, decisioni 28 agosto 2024, n. 9459 e 7 ottobre 2022, n. 12932; ABF, Collegio di Milano, dec. 24 aprile 2024, n. 4921.

(29) ABF, Collegio di Roma, dec. 2 aprile 2024, n. 3966.

(30) ABF, Collegio di Bologna, dec. 16 maggio 2024, n. 5880.

cliente, mediante l'impiego della diligenza del *bonus argentarius* (31); ossia una diligenza di natura tecnica che va valutata tenendo conto dei rischi tipici della sfera professionale di riferimento (32).

E ciò in quanto il fatto dell'eventuale uso da parte dei terzi dei codici di accesso al sistema potrebbe dirsi rientrare nell'alveo del rischio professionale del prestatore dei servizi di pagamento; rischio che, in qualche caso, potrebbe dirsi prevedibile ed evitabile con appropriate misure tecniche volte a verificare la riferibilità delle operazioni alla volontà del correntista. In questa direzione, la banca non risponde del danno patito dal cliente qualora dimostri che il fatto sia attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo (33).

In questa materia assume rilievo la funzione assolta dal servizio di « *sms-alert* ». Si tratta di una funzione protettiva che costituisce un presidio a tutela della trasparenza, della consapevolezza e della sicurezza dei pagamenti (34). In particolare, nel contesto delle frodi come quelle denominate di « *social hacking* », perpetrate non grazie ad una falla del sistema informatico dell'intermediario, ma attraverso la manipolazione psicologica del cliente, l'*sms-alert* può rappresentare uno strumento capace di richiamarne la sua attenzione in ordine alla reale natura dell'operazione che va compiendo, al fine di annullarla (35).

---

(31) F. Marasà, *Utilizzo fraudolento di carta bancomat e diligenza professionale della banca*, in *Banca. borsa tit. cred.*, 2016, 396 ss.

(32) Cass., sez. I, 12 giugno 2007, n. 1377; Cass., sez. I, 3 febbraio 2017, n. 2950; R. Frau, *Home banking, captazione di codici di accesso ed esclusione della responsabilità della banca*, in *Resp. civ. prev.*, 2024, 163. La diligenza posta a carico dell'istituto bancario ha natura tecnica e deve essere valutata ai sensi dell'art. 1176, comma 2, c.c., tenendo conto dei rischi tipici della sfera professionale di riferimento, assumendo come parametro la figura dell'accorto banchiere: spetta pertanto all'intermediario bancario provare di aver adottato tutte le misure idonee a garantire la sicurezza del servizio da eventuali manomissioni.

(33) App. Firenze, 8 settembre 2022. Nel caso di specie, la Corte ha confermato la condanna di una banca al risarcimento del danno a favore di un proprio correntista vittima di *phishing*, non avendo la prima fornito prova di aver adottato sistemi di sicurezza aggiuntivi, quali il servizio di « *sms alert* », tali da consentire l'immediato controllo da parte del cliente della propria operatività sul conto e quindi la revoca dell'operazione, disposta per errore o in modo fraudolento.

(34) ABF, Collegio di Bari, dec. 17 ottobre 2023, n. 10010; ABF, Collegio di Bari, dec. 27 novembre 2023, n. 11595; ABF, Collegio di Bari, dec. 5 luglio 2024, n. 7749; L. Muttini, *Frodi informatiche e responsabilità della banca: i nuovi orientamenti dell'arbitro bancario finanziario*, in *Riv. dir. banc.*, 2021, 41.

(35) ABF, Collegio di Milano, dec. 28 settembre 2023, n. 9367. Si v. inoltre ABF, Collegio di Bologna, dec. 5 giugno 2024, n. 6686, nella quale si legge: « l'intermediario non ha dimostrato di aver inviato rispetto a ciascuna di dette operazioni un *sms-alert* che se ricevuto dalla cliente avrebbe, con ogni probabilità, permesso alla stessa di chiedere tempestivamente

In particolare, il Collegio di coordinamento ABF ha posto in rilievo che « Anche nel caso in cui venga esclusa la clonazione dello strumento di pagamento, la mancata prova dell'attivazione del servizio di *sms alert* da parte dell'intermediario rappresenta una violazione al corretto adempimento degli obblighi posti a suo carico » (36).

L'attivazione del servizio di *sms alert* rientra, quindi, tra i doveri posti a carico del prestatore dei servizi di pagamento. La mancata attivazione di detto servizio costituisce pertanto una carenza organizzativa di regola imputabile all'intermediario, che non implica una sua responsabilità solo quando il cliente ad es. gli abbia rilasciato una specifica dichiarazione liberatoria al riguardo o abbia rinunciato alla facoltà di avvalersene (37).

Deve dirsi parimenti non imputabile all'intermediario il danno patito dal titolare dello strumento di pagamento in seguito ad un'operazione disconosciuta, risultata correttamente autenticata, approvata e contabilizzata (art. 10, comma 1, d.lgs. 27 gennaio 2010, n. 11), tutte le volte in cui, tenuto conto del contesto temporale nel quale si è consumata la frode (ad es., bonifico istantaneo fraudolento, eseguito immediatamente prima o dopo l'*sms alert*) o altrimenti (ad es., furto o mancata disponibilità del *device* sul quale avrebbe dovuto essere recapitato l'*sms*), il messaggio di allerta non avrebbe comunque potuto impedirla. In questi casi difetterebbe, infatti, qualunque nesso di causalità tra il mancato invio dell'*sms* e la frode (38).

6. *Segue*: *b*) gli indici di anomalia dell'operazione di pagamento.

È talvolta possibile ravvisare un concorso di colpa dell'intermediario anche nel caso in cui l'operazione di pagamento disconosciuta rientri in una delle fattispecie previste dal d.m. 30 aprile 2007, n. 112, recante il regola-

---

il blocco dello strumento di pagamento, così da impedire il compimento delle successive operazioni fraudolente ».

(36) ABF, Collegio di Coordinamento, dec. 23 luglio 2024, n. 8672.

(37) ABF, Collegio di Milano, decisioni 13 dicembre 2024, n. 12825 e 6 novembre 2019, n. 24366.

(38) Si v., ABF, Collegio di Torino, dec. 21 novembre 2024, n. 12066, nella quale si legge: « Per quel che concerne i doveri di protezione dell'utente gravanti sull'intermediario (trattasi, in particolare, dei servizi di *sms-alert* o assimilabili), secondo la posizione condivisa dei Collegi, che si fonda su un'interpretazione sostanzialistica, è irrilevante la mancata attivazione ovvero il mancato funzionamento del servizio di *sms-alert* (o di servizio assimilabile) nei casi in cui la ricezione dell'*alert* non possa in concreto limitare il pregiudizio dell'utente, ossia nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato. Nel caso in esame vi è un'unica operazione contestata, per cui il Collegio non ritiene la questione rilevante ».

mento di attuazione della l. 17 agosto 2005, n. 166, relativa all'« Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento ».

In particolare, ai sensi dell'art. 8, d.m. n. 112/2007 cit., rubricato *Rischio di frode*:

« 1. Si configura il rischio di frode di cui all'articolo 3, comma 1 della legge, quando viene raggiunto uno dei seguenti parametri:

a) con riferimento ai punti vendita di cui all'articolo 7, lettera *b*):

1) cinque o più richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita;

2) tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita;

3) richiesta di autorizzazione, approvata o rifiutata, che superi del 150% l'importo medio delle operazioni effettuate con carte di pagamento, nei tre mesi precedenti, presso il medesimo punto di vendita;

b) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'articolo 7, lettera *c*):

1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento;

2) una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento;

3) due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti ».

Quando un'operazione di pagamento può dirsi sospetta in base al citato art. 8, d.m. n. 112/2007, ecco che il cliente può essere ritenuto titolare del diritto di ottenere il rimborso della stessa operazione, oltreché di quelle successive, restando invece a suo carico il danno patito in conseguenza delle operazioni precedenti.

Occorre però formulare una duplice precisazione.

Innanzitutto, il fatto che l'operazione di pagamento possa qualificarsi come sospetta in quanto sussumile in una delle dette fattispecie non conduce necessariamente al sorgere del diritto al rimborso della stessa da parte della banca. Ciò in quanto, nonostante la natura sospetta dell'operazione, nel caso concreto potrebbe dirsi insussistente un profilo di colpa a carico della banca. Detto altrimenti, il d.m. del Ministero dell'Economia e delle Finanze 30 aprile 2007, n. 112 non ha valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate ([39]). Il diritto al rimborso dell'operazione sospetta è costituito solo in quanto l'indice di anomalia è tale da

([39]) ABF, Collegio di Milano, dec. 4 dicembre 2024, n. 12489.

richiamare l'attenzione dell'intermediario, nel senso di indurlo a bloccarla per ragioni di sicurezza (40).

Per converso, può anche darsi il caso di un'operazione che — quand'anche non riconducibile in una delle fattispecie previste dall'art. 8 cit. — sia, cionondimeno, oggettivamente sospetta, con conseguente diritto dell'utente ad ottenere il relativo rimborso per avere la banca omesso di dotarsi delle procedure necessarie a rilevarla e bloccarla. Si pensi, ad es., al caso di una serie di bonifici *online* eseguiti in rapida sequenza notte tempo, in alcun modo riconducibili alla normale operatività bancaria del cliente, magari fatti a valere su conti esteri, e che abbiano prodotto il pratico effetto dello svuotamento del conto corrente (41).

7. Il caso della « SIM *swap fraud* » e la posizione della giurisprudenza.

La « SIM *swap fraud* » è una tipologia di truffa informatica che consiste nell'impossessarsi del numero di cellulare dell'ignaro utente allo scopo di accedere ad una serie di servizi ed informazioni collegati alla SIM (42).

In particolare, come posto in rilievo dalla giurisprudenza, « la truffa del SIM *Swap* [...] opera su due fasi. La prima riguarda la captazione dei codici di identificazione o presso il correntista ingannandolo, il cosiddetto *phishing*, o con una intromissione illecita nel sistema informatico della banca o nel traffico telefonico dati/telefonico del correntista. [...] La seconda fase della truffa, essenziale per la sua riuscita, è quella dello scambio della sim. I truffatori riescono ad ottenere dal gestore telefonico [...] un duplicato della SIM del correntista bersaglio della truffa ed intercettando poi i codici inviati dalla banca per completare il pagamento » (43).

Sul tema si rileva un contrasto tra le decisioni dell'ABF e quelle della giurisprudenza di merito.

Secondo l'ABF, in caso di SIM *swap fraud*, le richieste di rimborso del danno proposte dal titolare dello strumento di pagamento nei confronti della banca devono dirsi — generalmente — meritevoli di accoglimento (44), in

(40) ABF, Collegio di Bologna, dec. 30 ottobre 2024, n. 11411.

(41) ABF, Collegio di Milano, dec. 2 dicembre 2024, n. 12379.

(42) « SIM » rappresenta l'acronimo di *Subscriber Identity Module*, tradotto letteralmente, « modulo di identificazione dell'utente », e rappresenta la *smart card* inserita nei dispositivi mobili che permette all'utente di connettersi a una rete cellulare e di effettuare chiamate o utilizzare i servizi di trasmissione dati.

(43) App. Genova, 13 dicembre 2024, n. RG 1140/2023, inedita.

(44) La truffa perpetrata con il metodo della SIM *swap fraud* comporta l'esclusione della colpa grave, posto che detta truffa risulta particolarmente sofisticata. In tal senso si veda ABF, Collegio di Milano, dec. 12 marzo 2021, n. 6758.

quanto la sostituzione della SIM card deve essere equiparata alla mancanza di autenticazione dell'operazione di pagamento *ex* art. 10 del d.lgs. 27 gennaio 2010, n. 11. La sostituzione della SIM, pur essendo riferibile ad un soggetto terzo (la compagnia telefonica), rientrerebbe per tale via nel rischio tipico dell'attività d'impresa dell'intermediario, che si avvale di una modalità di autenticazione (*sms*, otp) affidandola in parte a terzi (45).

Come accennato, la giurisprudenza ha però assunto una posizione diversa, tutta incentrata sul concetto di nesso di causalità tra condotta serbata dall'operatore telefonico e danno patito dal titolare dello strumento di pagamento (46). Secondo i giudici di merito, infatti, in questi casi, prima di procedere alla duplicazione della SIM richiesta dal malfattore, così come al successivo blocco della SIM precedente, la compagnia telefonica dovrebbe verificare l'identità del richiedente, nonché l'autenticità e l'attendibilità della denuncia di smarrimento presentata a tal fine. È solo l'assenza dei detti adempimenti a permettere ai malfattori di ottenere le credenziali dinamiche necessarie all'esecuzione dell'operazione illecita. L'effettuazione del bonifico fraudolento deve dirsi pertanto il « naturale » sviluppo dell'illecito SIM *Swap ex* art. 1223 c.c. (47).

La richiamata giurisprudenza ha, quindi, accertato una responsabilità esclusiva in capo all'operatore telefonico, per avere condotto una verifica dell'identità del richiedente la sostituzione solo superficiale e negligente, e risultata pertanto causa prima della successiva esecuzione dell'operazione fraudolenta (48).

---

(45) ABF, Collegio di Milano, dec. n. 2190/2024. Il Collegio precisa che: « Nel caso di specie, vengono fornite prove idonee a comprovare che la truffa presenti effettivamente i caratteri tipici c.d. « SIM *swap fraud* », attraverso la quale terzi soggetti trasferiscono l'utenza telefonica del titolare su una nuova SIM al fine di porre in essere un'operatività fraudolenta, ad esempio ricevendo le password dinamiche otp inviate a tale numero ».

(46) Trib. Napoli Nord, 30 dicembre 2024. Per una responsabilità concorrente tra intermediario e gestore telefonico cfr. Trib. Milano, 13 aprile 2022; Trib. Roma, 20 luglio 2023.

(47) App. Genova, 12 giugno 2024, n. RG 143/2023, inedita; App. Genova, 13 dicembre 2024, cit.; App. Genova, 12 febbraio 2025, Sez. III, n. RG 1141/2023, inedita.

(48) Cfr., Trib. Taranto, Sez. I, 5 aprile 2024, in *Quot. giur.*, 2024, secondo cui « In tema di c.d. SIM *swap fraud*, cioè la sottrazione di denaro attraverso l'ottenimento fraudolento del duplicato della SIM telefonica, è da escludere l'inadempimento contrattuale della banca qualora l'accesso al conto corrente del cliente sia dipeso esclusivamente dalla condotta colposa del gestore telefonico, il quale ha consentito, senza effettuare le opportune verifiche sull'identità del richiedente, la sostituzione della SIM ». Conformemente, si v. Trib. Roma, sez. XVI, 11 settembre 2023, n. 12832, in *Quot. giur.*, 2023, secondo cui « In tema di frodi informatiche compiute a danno della clientela bancaria attraverso la tecnica della c.d. SIM *swap fraud* che comporta prelievi illegittimi di denaro dal conto corrente, sussiste la responsabilità per

8. La spedizione della carta di pagamento. La tecnica del c.d. *boxing.*

Un altro profilo di responsabilità nel quale talvolta può incorrere l'intermediario è rappresentato dai casi di spedizione della carta di credito al cliente a mezzo del servizio postale (49).

Secondo l'orientamento dei Collegi ABF, sussiste infatti la responsabilità dell'intermediario quando la sottrazione dello strumento di pagamento, presupposto delle successive operazioni fraudolente, avvenga mediante la tecnica del c.d. *boxing*, ossia della illecita appropriazione della carta da parte di terzi nella fase di consegna al cliente, probabilmente in esito ad episodi di *social engineering* (50). In questi casi, l'allocazione del rischio della spedizione dello strumento di pagamento dipende da apposita previsione normativa, e, segnatamente, dall'art. 8, comma 2, del d.lgs. 27 gennaio 2010, n. 11, alla luce del quale i rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento.

Resta però ferma, in questi casi, la possibilità di valutare la concorrente colpa grave del titolare dello strumento di pagamento, il quale, nel momento in cui comunica ai malfattori le proprie credenziali di sicurezza, rende, in fin dei conti, possibile la consumazione della frode (51).

---

condotta negligente dell'operatore telefonico che abbia adottato una superficiale verifica dell'identità del richiedente la sostituzione della SIM ».

(49) Sul tema si veda G. Liberati Buccianti, *Carte di pagamento e (in)debiti utilizzi nelle decisioni dell'Arbitro Bancario Finanziario*, in *I contratti bancari*, a cura di C.M. Bianca, Roma, Dike, 2013, 55.

(50) ABF, Collegio di Bologna, dec. n. 1918/2023.

(51) Si v. ABF, Collegio di Napoli, dec. n. 9104/2023, nella quale si legge: « L'intermediario ha già riconosciuto la propria responsabilità nell'aver agevolato la produzione del danno mediante l'invio via posta ordinaria della nuova carta di pagamento; tuttavia, nel caso specifico, il rinnovo dello strumento di pagamento non ha comportato l'attribuzione di un nuovo pin (art. 16 delle Condizioni Contrattuali); è provato, infatti, che tutte le operazioni poi disconosciute sono state eseguite con la digitazione del vecchio pin, di cui i truffatori si sono impossessati mediante l'invio a parte ricorrente di *sms* con un link che il cliente, come espressamente riconosciuto, ha appunto comunicato il pin ai truffatori, con ciò contribuendo, con il proprio comportamento colposo, alla produzione del danno in misura del 50% dell'importo complessivo delle operazioni fraudolente ».

