Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro designato da Associazione rappresentativa degli intermediari
(MI) AFFERNI	Membro designato da Associazione rappresentativa dei clienti

Relatore AFFERNI

Nella seduta del 18/06/2024

- dopo aver esaminato l'istanza di correzione del dispositivo della decisione n. 6416/24 del 30/05/2024 presentata dalla ricorrente;
- viste le vigenti "Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari";

PREMESSO CHE

Nella riunione del 13/05/2024 il Collegio così decideva:

"*FATTO*

Parte ricorrente afferma che: era in attesa di ricevere un nuovo strumento di pagamento da parte dell'intermediario, poi sottratto da terzi ignoti al vettore incaricato del trasporto; in data 11/07/2023, alle ore 13:53, veniva apparentemente contattata telefonicamente dall'intermediario per confermare l'indirizzo di spedizione della carta; durante la telefonata riceveva un SMS che compariva nel canale di messaggistica ufficiale dell'intermediario, dal tenore genuino e privo di errori grammaticali, contenente un LINK con la denominazione dell'intermediario e dotato del protocollo "https" sicuro, oltre che la dicitura "/carte"; il LINK rinviava ad una schermata identificata con quella della banca, nella quale si richiedeva l'inserimento delle credenziali di accesso per l'autenticazione; accortasi della truffa, contattava tempestivamente alle ore 14:07 l'intermediario al fine di bloccare la carta e il conto e disconoscere l'operatività illecita, senza successo; la sottrazione della carta durante la spedizione ha consentito ai truffatori di conoscere il codice CVV della carta, richiesto nella fase di attivazione nell'area riservata dell'internet banking, oltre alla conoscenza di altri dati utili per rendere credibile la truffa (come l'indirizzo di consegna

della ricorrente); la responsabilità per la vicenda in esame è esclusivamente in capo all'intermediario; il vettore ha dichiarato in data 18/07/2023 alle ore 13:29 di aver smarrito la corrispondenza e, dunque, tardivamente, a distanza di una settimana dall'utilizzo illecito della carta; qualora il vettore avesse rilevato tempestivamente lo smarrimento, avrebbe impedito la frode; l'intermediario, fornitore dello strumento di pagamento, avrebbe dovuto rilevare l'anomalia dell'operazione disposta in località di Napoli, mentre la cliente è residente in provincia di Treviso ove attendeva la spedizione della carta; è stato integrato il parametro di rischio frode ex art. 8, D.M. 30 aprile 2007, n. 12 in quanto, come evincibile dal sito internet dell'intermediario, lo strumento di pagamento in esame ha un plafond di € 1.500,00 mensile, corrispondente all'importo della prima operazione contestata; solamente (circa) quindici giorni dopo l'illecito riceveva una Email dalla banca che avvisava la clientela di frodi come quella in esame; è stata vittima di una frode sofisticata, ovvero di Caller ID e SMS Spoofing, contraffazione del sito della banca e Social Engineering.
Parte ricorrente – esperita senza successo la fase del reclamo – chiede il rimborso della somma di € 1.500,00.
L'intermediario, con le controdeduzioni, precisa che: la ricorrente è stata vittima di boxing misto a social engineering; l'operatività contestata è stata correttamente contabilizzata, registrata e autenticata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; il frodatore, dopo aver intercettato materialmente la carta in corso di spedizione, ha ottenuto il PIN tramite il contatto telefonico e, sulla scorta di tale informazione, ha potuto attivare lo strumento di pagamento e, successivamente, validare le operazioni dispositive; la ricorrente ha altresì ricevuto le notifiche ALERT relative all'attivazione della propria Carta di Credito, a mezzo SMS ed Email, nonché quelle relative alla conferma di visualizzazione del PIN, sempre a mezzo Email, oltre che dell'operazione oggetto di disconoscimento (a mezzo push ed Email); ciononostante non si è insospettita e non ha posto immediato termine alla conversazione in corso; sussiste la colpa grave della cliente che ha dato credito ad un estraneo, comunicando i propri codici personali e ha autorizzato l'attivazione della Carta di Credito e l'operazione di conferma visualizzazione Pin Carta; ha da tempo attivato una campagna antifrode a favore dei propri clienti, fornendo ampie informazioni su come riconoscere un attacco phishing e su come comportarsi.
L'intermediario chiede, pertanto, di respingere il ricorso perché infondato.
Parte ricorrente, in sede di repliche, afferma che: l'intermediario, a seguito del ricorso, ha disposto il riaccredito del 30% di quanto richiesto e pertanto la domanda si limita al rimborso della minor somma di € 1.050,00; i precedenti richiamati dall'intermediario non sono riferibili al caso di specie, nel quale peraltro la ricorrente ha reagito alla truffa in brevissimo tempo, contattando l'intermediario nel giro di pochi minuti; nei casi di cd. boxing misto a phishing, invece, i Collegi territoriali hanno riconosciuto un rimborso integrale; l'intermediario non formula nessuna osservazione quanto all'adeguatezza dello strumento di consegna postale, generalmente ritenuto non sicuro e non adeguato a marginalizzare il rischio di frode, salvo ritenerlo "diffuso nella prassi" (circostanza che avrebbe dovuto far adottare all'intermediario presidi di sicurezza adeguati o strumenti di consegna alternativi); l'operazione controversa rileva ex art. 8, D.M. 30 aprile 2007, n. 12, tenuto conto dell'anomalia dell'operazione in esame, corrispondente alla giacenza media annua del conto della ricorrente e sensibilmente più elevata rispetto alle altre operazioni eseguite con il medesimo strumento di pagamento; l'intermediario non ha prodotto LOG idonei a provare la SCA.

DIRITTO

La controversia sottoposta all'esame del Collegio verte sulla ormai nota questione del furto di strumenti di pagamento e sul rimborso di somme indebitamente sottratte a seguito di disposizioni fraudolentemente impartite.
L'operazione contestata da parte ricorrente (pagamento POS del 11/07/2023 per un importo di € 1.500,00) rientro nell'ambito di applicazione della disciplina del D. Lgs. 27/1/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
La normativa richiamata ha provveduto a ripartire una serie di obblighi tra il prestatore di servizi di pagamento e l'utilizzatore di detti servizi. L'utilizzatore, in particolare, ha il dovere di utilizzare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici PIN). Per quanto riguarda l'intermediario, la normativa ricordata prevede, tra gli altri, l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi.
Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.
La normativa mostra un chiaro favor probatorio nei confronti dell'utilizzatore, in quanto l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo oppure che questi abbia agito in modo fraudolento ovvero con dolo o colpa grave.
La ratio di tale scelta legislativa è 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 (cfr. Corte di Cassazione n. 9158/2018).
Alla luce di tali disposizioni, pertanto, due sono i passaggi ineludibili in materia. In primo luogo è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore (Collegio di Milano, decisione n. 1588 del 17 febbraio 2017). In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
Nel caso di specie, sotto il primo profilo, l'intermediario ha prodotto documentazione relativa alla registrazione, contabilizzazione e autenticazione delle operazioni disconosciute, assolvendo in questo modo il proprio onere probatorio di autenticazione ed esecuzione.
Può dirsi quindi raggiunta la prova, che grava sull'intermediario, richiesta dall'art. 10, comma primo, D.Lgs. n. 11/2010 cit. ed è pertanto possibile accedere alla valutazione del comportamento dell'utilizzatore ai fini dell'applicazione delle previsioni del successivo art. 12, terzo comma.
Si tratta, in particolare, di verificare se ricorra o meno una violazione degli obblighi di cui all'art. 7 D.Lgs. n. 11/2010 cit. imputabile ad un comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore.
L'indagine intorno alla sussistenza di tali elementi soggettivi – a parte le ipotesi di dolo – risulta particolarmente articolata con riguardo all'ipotesi, quale quella prospettata dall'intermediario nel caso in esame, di colpa grave dell'utilizzatore.

I vari Collegi ABF hanno chiarito, in conformità alle decisioni assunte dalla giurisprudenza di legittimità, che la colpa grave consiste in un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti: non dunque ogni contegno imprudente può far ritenere integrato questo grado di colpa, ma solo quello che appaia abnorme ed inescusabile (cfr. Collegio di Coordinamento, decisione n. 5304/2013).
Secondo quanto riferito dalla ricorrente in denuncia, nel reclamo e nel ricorso (e non contestato dall'intermediario resistente), si tratterebbe di un caso assimilabile al c.d. boxing (i truffatori intercettano e rubano la carta di pagamento spedita dall'emittente al titolare unitamente ai suoi dati personali), combinato con il c.d. spoofing: nel caso specifico il titolare dello strumento di pagamento, dopo aver ricevuto un SMS truffaldino, è stato contattato telefonicamente da un falso addetto dell'intermediario che, essendo in possesso dei suoi dati personali, si è guadagnato la sua fiducia estorcendogli verosimilmente il codice PIN.
Nel caso di specie si rileva che: la denominazione della chat in cui è inserito il messaggio civetta è riferibile all'intermediario convenuto; nella medesima chat sono presenti messaggi genuini dell'intermediario successivi a quello civetta (sms attivazione della carta); il messaggio civetta contiene un LINK che contiene un riferimento dell'intermediario e non contiene errori grammaticali e/o lessicali.
Il Collegio rileva altresì la mancata adozione di presidi di sicurezza idonei a evitare l'ingerenza di terzi nella sfera patrimoniale del cliente da parte dell'intermediario, sul quale grava il rischio di impresa derivante dalla spedizione dello strumento di pagamento.
Alla luce delle risultanze istruttorie, il Collegio ritiene che non siano emerse circostanze tali da far ritenere che vi sia stata in capo alla ricorrente una colpa grave.
Per quanto esposto, questo Collegio dispone a favore di parte ricorrente il rimborso della somma di € 1.050,00, pari all'ammontare dell'operazione disconosciuta, al netto dei rimborsi già effettuati.

PQM

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.050,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

Il Presidente"

***

Con istanza di correzione del 3 giugno 2024 parte ricorrente rileva un errore nel dispositivo della decisione, con riferimento all'ammontare della condanna. Ciò in quanto:

- l'intermediario ha dato evidenza del pagamento, a seguito della presentazione del ricorso, del 70% della somma richiesta (Euro 1.500,00), procedendo quindi a versare in favore della cliente l'importo di Euro 1.050,00;
- la richiesta della ricorrente, precisata in sede di repliche, è pari al rimanente 30%, e quindi ammonta a Euro 450,00;
- il dispositivo della pronuncia, invece, indica erroneamente la condanna dell'intermediario al rimborso dell'importo di Euro 1.050,00.

Parte ricorrente chiede quindi che l'importo della condanna sia contenuto nella somma

(corretta) di Euro 450,00, cui si aggiunge l'importo di Euro 200,00 da corrispondere alla Banca d'Italia, avendo l'intermediario restituito anche Euro 20,00 per spese di presentazione ricorso.

L'istanza coglie nel segno e va accolta.

Infatti è pacifico che l'importo di Euro 1.050,00 corrisponde, in realtà, a quanto già rimborsato dall'intermediario; è in atti l'evidenza contabile trasmessa dall'intermediario nel corso del procedimento che conferma il rimborso dell'importo di Euro 1.050,00, nonché del contributo di Euro 20,00 per la presentazione del ricorso ABF.

Per tali ragioni, in considerazione di quanto precede, il dispositivo risulta erroneo in quanto avrebbe dovuto limitarsi alla condanna alla restituzione dell'importo di Euro 450,00, oltre alla corresponsione solo di Euro 200,00 alla Banca d'Italia per le spese di procedura.

PER QUESTI MOTIVI

Il Collegio, ritenuta la fondatezza dell'istanza di correzione in quanto dagli atti risultava che l'intermediario avesse già corrisposto alla parte ricorrente la somma di € 1.050,00 nonché il contributo di spese pari a € 20,00, accoglie l'istanza e dispone che l'intermediario corrisponda alla parte ricorrente non già la somma di € 1.050,00 ma la somma di € 450,00 e che sia esonerato dal pagamento di € 20,00 a titolo di spese di procedura.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) GRIPPO

Seduta del 13/05/2024

FATTO

Parte ricorrente afferma che:

- era in attesa di ricevere un nuovo strumento di pagamento da parte dell'intermediario, poi sottratto da terzi ignoti al vettore incaricato del trasporto;
- in data 11/07/2023, alle ore 13:53, veniva apparentemente contattata telefonicamente dall'intermediario per confermare l'indirizzo di spedizione della carta;
- durante la telefonata riceveva un SMS che compariva nel canale di messaggistica ufficiale dell'intermediario, dal tenore genuino e privo di errori grammaticali, contenente un LINK con la denominazione dell'intermediario e dotato del protocollo "https" sicuro, oltre che la dicitura "/carte";
- il LINK rinviava ad una schermata identificata con quella della banca, nella quale si richiedeva l'inserimento delle credenziali di accesso per l'autenticazione;
- accortasi della truffa, contattava tempestivamente alle ore 14:07 l'intermediario al fine di bloccare la carta e il conto e disconoscere l'operatività illecita, senza successo;
- la sottrazione della carta durante la spedizione ha consentito ai truffatori di conoscere il codice CVV della carta, richiesto nella fase di attivazione nell'area riservata dell'internet banking, oltre alla conoscenza di altri dati utili per rendere credibile la truffa (come l'indirizzo di consegna della ricorrente);

- la responsabilità per la vicenda in esame è esclusivamente in capo all'intermediario;
- il vettore ha dichiarato in data 18/07/2023 alle ore 13:29 di aver smarrito la corrispondenza e, dunque, tardivamente, a distanza di una settimana dall'utilizzo illecito della carta;
- qualora il vettore avesse rilevato tempestivamente lo smarrimento, avrebbe impedito la frode;
- l'intermediario, fornitore dello strumento di pagamento, avrebbe dovuto rilevare l'anomalia dell'operazione disposta in località di Napoli, mentre la cliente è residente in provincia di Treviso ove attendeva la spedizione della carta;
- è stato integrato il parametro di rischio frode *ex* art. 8, D.M. 30 aprile 2007, n. 12 in quanto, come evincibile dal sito internet dell'intermediario, lo strumento di pagamento in esame ha un plafond di € 1.500,00 mensile, corrispondente all'importo della prima operazione contestata;
- solamente (circa) quindici giorni dopo l'illecito riceveva una Email dalla banca che avvisava la clientela di frodi come quella in esame;
- è stata vittima di una frode sofisticata, ovvero *di Caller ID* e *SMS Spoofing*, contraffazione del sito della banca e Social Engineering.

Parte ricorrente – esperita senza successo la fase del reclamo – chiede il rimborso della somma di € 1.500,00.

L'intermediario, con le controdeduzioni, precisa che:

- la ricorrente è stata vittima di *boxing* misto a *social engineering*;
- l'operatività contestata è stata correttamente contabilizzata, registrata e autenticata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
- il frodatore, dopo aver intercettato materialmente la carta in corso di spedizione, ha ottenuto il PIN tramite il contatto telefonico e, sulla scorta di tale informazione, ha potuto attivare lo strumento di pagamento e, successivamente, validare le operazioni dispositive;
- la ricorrente ha altresì ricevuto le notifiche ALERT relative all'attivazione della propria Carta di Credito, a mezzo SMS ed Email, nonché quelle relative alla conferma di visualizzazione del PIN, sempre a mezzo Email, oltre che dell'operazione oggetto di disconoscimento (a mezzo push ed Email);
- ciononostante non si è insospettita e non ha posto immediato termine alla conversazione in corso;
- sussiste la colpa grave della cliente che ha dato credito ad un estraneo, comunicando i propri codici personali e ha autorizzato l'attivazione della Carta di Credito e l'operazione di conferma visualizzazione Pin Carta;
- ha da tempo attivato una campagna antifrode a favore dei propri clienti, fornendo ampie informazioni su come riconoscere un attacco *phishing* e su come comportarsi.

L'intermediario chiede, pertanto, di respingere il ricorso perché infondato.

Parte ricorrente, in sede di repliche, afferma che:

- l'intermediario, a seguito del ricorso, ha disposto il riaccredito del 30% di quanto richiesto e pertanto la domanda si limita al rimborso della minor somma di € 1.050,00;

- i precedenti richiamati dall'intermediario non sono riferibili al caso di specie, nel quale peraltro la ricorrente ha reagito alla truffa in brevissimo tempo, contattando l'intermediario nel giro di pochi minuti;
- nei casi di cd. *boxing* misto a *phishing*, invece, i Collegi territoriali hanno riconosciuto un rimborso integrale;
- l'intermediario non formula nessuna osservazione quanto all'adeguatezza dello strumento di consegna postale, generalmente ritenuto non sicuro e non adeguato a marginalizzare il rischio di frode, salvo ritenerlo "diffuso nella prassi" (circostanza che avrebbe dovuto far adottare all'intermediario presidi di sicurezza adeguati o strumenti di consegna alternativi);
- l'operazione controversa rileva *ex* art. 8, D.M. 30 aprile 2007, n. 12, tenuto conto dell'anomalia dell'operazione in esame, corrispondente alla giacenza media annua del conto della ricorrente e sensibilmente più elevata rispetto alle altre operazioni eseguite con il medesimo strumento di pagamento;
- l'intermediario non ha prodotto LOG idonei a provare la SCA.

DIRITTO

La controversia sottoposta all'esame del Collegio verte sulla ormai nota questione del furto di strumenti di pagamento e sul rimborso di somme indebitamente sottratte a seguito di disposizioni fraudolentemente impartite.
L'operazione contestata da parte ricorrente (pagamento POS del 11/07/2023 per un importo di € 1.500,00) rientro nell'ambito di applicazione della disciplina del D.Lgs. 27/1/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
La normativa richiamata ha provveduto a ripartire una serie di obblighi tra il prestatore di servizi di pagamento e l'utilizzatore di detti servizi. L'utilizzatore, in particolare, ha il dovere di utilizzare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici PIN). Per quanto riguarda l'intermediario, la normativa ricordata prevede, tra gli altri, l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi.
Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.
La normativa mostra un chiaro *favor* probatorio nei confronti dell'utilizzatore, in quanto l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo oppure che questi abbia agito in modo fraudolento ovvero con dolo o colpa grave.
La *ratio* di tale scelta legislativa è 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 (cfr. Corte di Cassazione n. 9158/2018).
Alla luce di tali disposizioni, pertanto, due sono i passaggi ineludibili in materia. In primo luogo, è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova che comunque di per sé non è

sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore (Collegio di Milano, decisione n. 1588 del 17 febbraio 2017). In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.

Nel caso di specie, sotto il primo profilo, l'intermediario ha prodotto documentazione relativa alla registrazione, contabilizzazione e autenticazione delle operazioni disconosciute, assolvendo in questo modo il proprio onere probatorio di autenticazione ed esecuzione.

Può dirsi quindi raggiunta la prova, che grava sull'intermediario, richiesta dall'art. 10, comma primo, D.Lgs. n. 11/2010 cit. ed è pertanto possibile accedere alla valutazione del comportamento dell'utilizzatore ai fini dell'applicazione delle previsioni del successivo art. 12, terzo comma.

Si tratta, in particolare, di verificare se ricorra o meno una violazione degli obblighi di cui all'art. 7 D.Lgs. n. 11/2010 cit. imputabile ad un comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore.

L'indagine intorno alla sussistenza di tali elementi soggettivi – a parte le ipotesi di dolo – risulta particolarmente articolata con riguardo all'ipotesi, quale quella prospettata dall'intermediario nel caso in esame, di colpa grave dell'utilizzatore.

I vari Collegi ABF hanno chiarito, in conformità alle decisioni assunte dalla giurisprudenza di legittimità, che la colpa grave consiste in un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti: non dunque ogni contegno imprudente può far ritenere integrato questo grado di colpa, ma solo quello che appaia abnorme ed inescusabile (cfr. Collegio di Coordinamento, decisione n. 5304/2013).

Secondo quanto riferito dalla ricorrente in denuncia, nel reclamo e nel ricorso (e non contestato dall'intermediario resistente), si tratterebbe di un caso assimilabile al c.d. *boxing* (i truffatori intercettano e rubano la carta di pagamento spedita dall'emittente al titolare unitamente ai suoi dati personali), combinato con il c.d. *spoofing*: nel caso specifico il titolare dello strumento di pagamento, dopo aver ricevuto un SMS truffaldino, è stato contattato telefonicamente da un falso addetto dell'intermediario che, essendo in possesso dei suoi dati personali, si è guadagnato la sua fiducia estorcendogli verosimilmente il codice PIN.

Nel caso di specie si rileva che:

- la denominazione della chat in cui è inserito il messaggio civetta è riferibile all'intermediario convenuto;
- nella medesima chat sono presenti messaggi genuini dell'intermediario successivi a quello civetta (sms attivazione della carta);
- il messaggio civetta contiene un LINK che contiene un riferimento dell'intermediario e non contiene errori grammaticali e/o lessicali.

Il Collegio rileva altresì la mancata adozione di presidi di sicurezza idonei a evitare l'ingerenza di terzi nella sfera patrimoniale del cliente da parte dell'intermediario, sul quale grava il rischio di impresa derivante dalla spedizione dello strumento di pagamento.

Alla luce delle risultanze istruttorie, il Collegio ritiene che non siano emerse circostanze tali da far ritenere che vi sia stata in capo alla ricorrente una colpa grave.

Per quanto esposto, questo Collegio dispone a favore di parte ricorrente il rimborso della somma di € 1.050,00, pari all'ammontare dell'operazione disconosciuta, al netto dei rimborsi già effettuati.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.050,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA