diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

# Quali tutele per l'utente nelle operazioni di pagamento elettronico?

**Autore**: Redazione
**In**: Diritto civile e commerciale

**La disciplina prevista nel d.lgs. 11 del 2010**

Il d.lgs. n. 11 del 2010 (di attuazione della Direttiva n. 2007/64/CE, cosiddetta PSD e recentemente modificato dal d.lgs. 218/2017, di attuazione della Direttiva n. 2015/2366, cosiddetta PSD2) individua gli obblighi esistenti in capo al prestatore di servizi di pagamento, in relazione agli **strumenti di pagamento**, e le responsabilità per operazioni non autorizzate e per l'utilizzo non autorizzato di strumenti o servizi di pagamento.

L'art. 8 del decreto pone in capo al prestatore di servizi di pagamento il compito di impedire l'accesso a terzi ai dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento (fatti salvi, però, gli obblighi posti in capo, dall'art. 7, all'utente abilitato: cioè l'utilizzo degli strumenti di pagamento in conformità alle disposizioni contrattuali, l'adozione di misure idonee a proteggere le credenziali di sicurezza personalizzate e la comunicazione senza indugio, appena ne viene a conoscenza, dello smarrimento, furto o uso non autorizzato dello strumento).

L'art. 10 dispone che qualora l'utente di un servizio di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita oppure sostenga che questa non sia stata eseguita correttamente, incombe sul prestatore di servizi di pagamento (e, se l'operazione è disposta mediante un prestatore di **servizi di disposizione di ordine di pagamento** – soggetto, questi, che si frappone tra il pagatore ed il suo conto di pagamento online, disponendo l'ordine di pagamento verso una terza parte beneficiaria – incombe, su quest'ultimo, nell'ambito delle proprie competenze) provare che, invece, l'operazione è stata correttamente effettuata ("autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti"). Pertanto, all'utente è sufficiente disconoscere il pagamento, negando di averlo autorizzato. Spetta al prestatore dei servizi di pagamento (ad esempio, alla Banca) e, se del caso, al prestatore dei servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente.

La colpa grave può ravvisarsi in un comportamento 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" (Cass., n. 14456/2001). L'art. 11 dispone che in caso di operazione di


*Diritto & Diritti ISSN 1127-8579*

pagamento non autorizzata venga immediatamente rimborsato al pagatore l'importo dell'operazione. L'art. 12, invece, esclude che l'utente possa sopportare le perditi derivanti dall'utilizzo di uno strumento di pagamento smarrito, sottratto, utilizzato dopo la comunicazione, eseguita ai sensi del citato art. 7 (salvo il caso in cui l'utente abbia agito in modo fraudolento o non abbia adempiuto, con dolo o colpa gravi, agli obblighi di cui allo stesso art. 7). Tuttavia, l'utente (o, meglio, il pagatore) può sopportare personalmente la perdita subita, a titolo di "franchigia", sino ad euro 50 (l'originale importo di 150 euro è stato ridotto dal d.lgs. n. 218 del 2017).

## Le frodi più frequenti

Le frodi più frequenti riguardanti le carte di credito e consistenti nella sottrazione di somme dal conto del malcapitato, sono quelle denominate "**Frodi Card not present**". Questo perché, per la loro realizzazione, non richiedono la disponibilità materiale della carta e neppure l'apposizione della firma del titolare. Si tratta di operazioni generalmente effettuate per via telematica utilizzando i dati della carta di pagamento, cioè le generalità del titolare, il numero della carta, la data di scadenza e il codice CVV. I sistemi utilizzati dai truffatori per appropriarsi dei dati personali necessari sono i più vari e fantasiosi. Il più diffuso è il "phishing". Chi lo mette in pratica non si serve di tecnologie sofisticate (tipo virus, spyware o malware) ma si limita a ... chiedere alla potenziale vittima le informazioni necessarie!

La tecnica preferita consiste nell'inviare normali e-mail, generalmente riportanti il logo contraffatto di una Banca o di servizi di pagamento online, invitando il destinatario a fornire dati riservati, quali numero del conto corrente, dati della carta di credito, password e codici di accesso, ecc., motivando la richiesta con le più diverse ma apparentemente verosimili ragioni (ad esempio, la scadenza della password, il potenziale rinnovo della carta di pagamento, problemi di natura tecnica, la incompleta o errata presenza di informazioni da completare o correggere, ecc.). Il termine "phishing", del resto, deriva dalla parola inglese "fishing", che significa "pescare" e rende molto bene l'idea di chi cerca di "pescare", nel mare di internet, ingenui utenti per carpire loro preziose informazioni personali. Tecnica meno diffusa è, invece, l'**invio di SMS ingannevoli** (in questo caso si parla di "smishing").

Altro sistema praticato è quello denominato "skimming". In questo caso vengono acquisiti i dati contenuti nella banda magnetica della carta per essere copiati su una carta falsa (caso classico di "clonazione" di carta). L'acquisizione dei dati avviene presso l'esercizio commerciale dove il titolare della carta effettua una transazione. La carta, dopo essere stata regolarmente "passata" nel POS, senza che il titolare della stessa se ne accorga viene "passata" in uno skimmer, cioè in un apparecchio (di ridottissime dimensione) in grado di catturare i dati contenuti nella banda magnetica. Per fortuna, in seguito alla adozione sulle carte di microchip (che garantiscono una maggiore sicurezza), è una truffa ormai in via di estinzione.

Il "trashing", invece, è un sistema che si basa sugli scontrini delle carte di credito e che, sovente, vengono imprudentemente gettati dopo la transazione. Dagli scontrini è possibile, infatti, acquisire dati personali


*Diritto & Diritti ISSN 1127-8579*

sufficienti per la creazione di una carta clonata. Altri metodi sono lo “sniffing”, con cui vengono intercettate le coordinate delle transazioni effettuate on line e il “boxing”, consistente nella clonazione delle carte di credito inviate dalle banche al domicilio del cliente (previa sottrazione della busta contenente la carta dalla cassetta delle lettere; busta e carta che, dopo la clonazione, vengono ricollocate nella buca delle lettere; il tutto all’insaputa della vittima). Numerose, poi, le frodi che vengono compiute presso gli sportelli ATM. Nella maggior parte dei casi, per poter clonare la carta, viene applicato un lettore di banda magnetica sopra o all’interno del vero lettore di carta. Spesso viene abbinato, allo scopo di individuare il PIN, ad una piccola videocamera nascosta oppure ad una finta tastiera numerica applicata su quella originale.

**Il presente contributo è trattato**

https://www.diritto.it/quali-tutele-lutente-nelle-operazioni-pagamento-elettronico/



*Diritto & Diritti ISSN 1127-8579*