Condizioni particolari per la Procedura 3D Secure nelle Operazioni Online mediante Carte di Pagamento

Le seguenti Condizioni Particolari si applicano in aggiunta alle Condizioni Generali per la Prestazione di Servizi Bancari e di Pagamento di Solarisbank AG, Succursale Italiana (di seguito: la "**Banca**") e alle Condizioni Particolari per il Canale di Online Banking e disciplinano la Procedura 3D Secure per le operazioni online con carte di pagamento emesse dalla Banca.

1. Oggetto, Definizione

(1) La Banca permette ai titolari di carte abilitate all'utilizzo online di partecipare alla procedura 3D Secure, eventualmente prevista dagli operatori di e-commerce.
(2) La procedura 3D Secure (denominata presso MasterCard come "MasterCard Identity Check" e presso VISA come "VISA SECURE") è una procedura di autenticazione in operazioni online mediante carte di pagamento.
(3) Ai fini dell'autorizzazione di operazioni online mediante carte di pagamento il/la titolare della carta deve utilizzare determinati elementi di autenticazione indicati nelle Condizioni Particolari per il Canale di Online Banking.
(4) Tali elementi di autenticazione sono ad esempio un numero trasmesso via SMS (Short Message Service) al/la titolare della carta di pagamento dalla Banca (di seguito "mobileTAN"); l'autenticazione In-App, nella quale il/la titolare della carta di pagamento viene reindirizzato all'applicazione banking del partner della Banca (di seguito "autenticazione In-App"); oppure domande di sicurezza a cui è in grado di rispondere solo il/la titolare della carta.
(5) La Banca ha il diritto di rifiutare l'esecuzione di un'operazione su internet nel caso in cui gli operatori di e-commerce non partecipino alla procedura 3D Secure.

2. Presupposti di partecipazione

(1) Ogni titolare di una carta di pagamento in corso di validità e che non è stata bloccata partecipa automaticamente alla procedura 3D Secure. L'iscrizione avviene all'attivazione della carta. Non è necessaria alcuna registrazione separata.
(2) Per poter procedere durante un pagamento mediante carta tramite 3D Secure a mezzo di autenticazione mobileTAN, il/la titolare della carta deve aver depositato presso la Banca attraverso il proprio partner un numero di telefono. Tale numero è modificabile in ogni momento.
(3) Al fine dello svolgimento di un'autenticazione 3D Secure mediante autenticazione In-App il/la titolare deve aver collegato con successo il proprio dispositivo mobile al conto relativo alla carta di pagamento utilizzata.

3. Autenticazione a mezzo 3D Secure

(1) Il mobileTAN trasmesso via SMS consiste in almeno sei caratteri e/o cifre da inserire al fine dell'autenticazione dell'operazione online mediante carta di pagamento. Per permettere un riscontro, sono mostrate sullo schermo al/la titolare della carta le ultime cifre del numero di telefono mobile fornito alla Banca.
(2) L'SMS viene messo a disposizione gratuitamente dalla Banca.
(3) Al fine dell'autenticazione In-App il/la titolare della carta deve accedere all'applicazione banking del partner di cooperazione della Banca su cui viene reindirizzato/a e confermare l'operazione online.
(4) Ai fini dell'autenticazione mediante risposta ad una domanda di sicurezza, il/la titolare della carta deve rispondere ad una domanda di cui solo lui/lei conosce la risposta.

4. Doveri di diligenza del/la titolare della carta

(1) Il/la titolare della carta deve assicurarsi che nessun terzo possa avere accesso al suo dispositivo mobile per eseguire operazioni online. La Banca non richiederà al/la titolare della carta la registrazione ovvero la comunicazione dei propri dati di registrazione né via e-mail né telefonicamente.
(2) Il/la titolare deve porre in essere idonee misure di sicurezza per proteggere gli SMS che vengono ricevuti sul dispositivo mobile (ad esempio mediante l'accesso consentito solamente tramite password). La Banca non è responsabile ove, a causa di furto, smarrimento o consegna a terzi del dispositivo mobile, terzi eventualmente riescano ad a accedere agli SMS e facciano uso del loro contenuto. Ciò vale anche per gli elementi di autenticazione che vengono utilizzati per l'accesso all'applicazione banking del partner della Banca.
(3) Il/la titolare della carta deve verificare la corrispondenza dei dati a lui/lei trasmessi via SMS (cfr. Articolo 3.2). In caso di mancata corrispondenza, l'operazione deve essere interrotta e la Banca ne deve essere informata.

5. Trattamento dei dati e fornitori di servizi

(1) Nel caso di pagamento mediante carta 3D Secure sono salvati il numero della carta, la data e l'orario di esecuzione, l'importo dell'operazione, le informazioni dell'operatore (Nome, ID, URL), nonché l'indirizzo IP da cui è stato eseguito l'ordine.
(2) La Banca è autorizzata ad incaricare fornitori di servizi per lo svolgimento della procedura 3D Secure. La Banca mette a disposizione di tali fornitori di servizi dati personali (ad esempio il numero della carta di credito) del/la titolare della carta esclusivamente per le finalità di esecuzione del contratto.