Digital Payments
for a Trusted World

WORLDLINE

Consigli di sicurezza per Mail/Phone Order

L'uso fraudolento dei numeri delle carte di pagamento nella vendita a distanza ogni anno causa danni notevoli che, a loro volta, sono all'origine di elevati oneri amministrativi. Le seguenti informazioni vi aiuteranno a proteggervi meglio dai truffatori.

I truffatori agiscono spesso seguendo lo stesso modus operandi:

- Una grossa ordinazione viene effettuata per fax, e-mail o telefono. La merce deve essere fornita immediatamente, per corriere espresso oppure postale con spese a carico dell'ordinante. Nella maggior parte dei casi l'indirizzo di consegna si trova all'estero oppure la fornitura viene richiesta presso un hotel o con fermo posta.
- Il pagamento, molto spesso, viene richiesto sia suddiviso con diverse carte di pagamento.

Secondo le disposizioni contrattuali in vigore per i pagamenti a distanza, per ogni singola transazione va sempre richiesta una autorizzazione. Tuttavia, l'autorizzazione è atta unicamente a verificare la validità e la solvibilità della carta in quel determinato momento.

Non è quindi possibile accertare in modo definitivo se colui che ha effettuato l'ordine sia di fatto il legittimo titolare della carta o se, invece, si tratti di un'altra persona che, in possesso dei suoi dati personali e della sua carta di pagamento stia tentando di agire in modo fraudolento.

Per tale motivo, le società di carte declinano qualsiasi responsabilità in relazione alle ordinazioni per fax o telefono.

VI ASSUMETE APPIENO IL RISCHIO

Mentre il truffatore ha ricevuto la merce, il legittimo titolare della carta contesta l'addebito del relativo importo. Per il partner contrattuale coinvolto ciò comporta spesso conseguenze particolarmente spiacevoli: da un lato, la sua merce è andata persa e, dall'altro, l'importo complessivo della transazione verrà riaddebitato.

Alcune raccomandazioni per minimizzare il rischio:

1. ACCETTAZIONE DELLE CARTE

Secondo il contratto d'accettazione delle carte, gli ordini possono essere accettati esclusivamente per fax, telefono o tramite il negozio online. Se ricevete ordini tramite e-mail che contengono i dati delle carte, dovrete informare il mittente che questa modalità non è ammessa.

Prima di rispondere al mittente ricordate di cancellare i dati della carta indicati nell'e-mail e da qualsiasi eventuale archivio elettronico. Quindi, stampate l'e-mail ed eliminatela sia dalla «Posta in entrata» come pure dalla cartella «Posta eliminata».

2. DATI DELLE CARTE IN FORMA CARTACEA

Assicuratevi che i documenti cartacei su cui figurano i numeri integrali delle carte non siano mai lasciati incustoditi e siano eliminati in modo appropriato. Non gettate nel cestino dei rifiuti i documenti cartacei su cui sono indicati i numeri integrali delle carte che non vi occorrono più, ma distruggeteli tramite un tritacarta affinché sia impossibile risalire alle informazioni riportate originariamente.

Introducete una policy che preveda la conservazione dei dati delle carte solo per il minor tempo necessario, ed eliminate con l'appropriata cura man mano i documenti con i dati delle carte che non vi occorrono più.

3. TRASMISSIONE DEI NUMERI DELLE CARTE

Prima di trasmettere i dati delle carte chiedetevi se il destinatario necessita veramente del numero integrale della stessa. Diversamente inviate il numero della carta rappresentato nel seguente formato: xxxx xxxx xxxx 1234. Questa rappresentazione del numero di carta è denominata PAN Truncation.

Evitate assolutamente di trasmettere i numeri delle carte tramite e-mail. Comunicate i dati delle carte per telefono o via fax.

4. ORDINI VIA INTERNET

Consigliamo ai gestori di negozi online di implementare una soluzione di sicurezza 3-D Secure 2 (per es. «Visa Secure» o «Mastercard Identity Check»). Questo procedimento consente di ridurre notevolmente il rischio di frodi trasferendo, la responsabilità sull'emittente della carta in caso comunque si verificasse una frode.

Se avete un vostro modulo d'ordine, assicuratevi che soddisfi gli obblighi imposti dallo standard PCI DSS (per es. nessuna richiesta di CVC2/CVV2). E' necessario monitorare in modo costante il processo d'ordine se contenga anche i dati delle carte, così come la loro eventuale (temporanea) archiviazione.

Come alternativa sicura all'accettazione degli ordini via fax, via e-mail o per telefono, vi consigliamo di integrare la nostra soluzione pay per link Secure PayGate. Con qualche piccola modifica potrete beneficiare di moduli conformi allo standard PCI e dei vantaggi di 3-D Secure 2.

5. VERIFICATE L'ORDINE

Prestate la massima attenzione in caso di ordinazioni ravvicinate di quantità e importi inusuali o da indirizzi e-mail di provider gratuiti, come yahoo.com, gmx.com o hotmail.com.

6. CONTROLLATE L'INDIRIZZO DI CONSEGNA

Controllate con attenzione l'indirizzo di consegna se fosse diverso da quello di residenza del cliente.

Vi sconsigliamo fortemente di effettuare consegne in Paesi in via di sviluppo, in particolare quelli dell'Africa, dell'Estremo Oriente, del Sud America nonché i paesi dell'ex Unione Sovietica, tranne nel caso sussista una relazione d'affari con clienti a voi ben noti.

Prestate particolare attenzione in caso di spedizioni a caselle postali o presso alberghi.

7. VALUTATE IL RISCHIO

Voi siete i nigliori conoscitori del vostro ambito commerciale e di come funzionano gli ordini. Se vi sorgessero delle perplessità, ma ugualmente aveste il desiderio di proseguire con la gestione dell'ordine, vi consigliamo di rivolgervi alla vostra banca di fiducia richiedendo informazioni in merito alla garanzia dei rischi legati alle esportazioni.

L'interlocutore locale è indicato su: worldline.com/merchant-services/contacts

110.0174.04 INT_IT/10.2021