

Porady dotyczące bezpieczeństwa przy zamówieniach drogą korespondencyjną/telefoniczną

Kradzieże lub bezprawne wykorzystywanie numerów kart co roku przynoszą pokaźne straty finansowe również w przypadku zamówień składanych drogą mailową/telefoniczną. Takie przypadki wiążą się z dużymi nakładami administracyjnymi. Poniższe informacje pomogą Państwu lepiej przeciwdziałać oszustwom z udziałem kart.

Oszuści często działają w oparciu o identyczny schemat:

- Faksem, e-mailem lub telefonicznie składane jest duże zamówienie. Zamówiony towar ma zostać jak najszybciej dostarczony przesyłką ekspresową lub kurierem na koszt zamawiającego. Adres dostawy to najczęściej adres zagraniczny. Często wymagana jest także dostawa do hotelu lub przesyłka „poste restante”.
- Płatność realizowana jest często kilkoma kartami.

Zgodnie z warunkami umowy transakcji na odległość przy każdej transakcji są Państwo zobowiązani do uzyskania autoryzacji. W trakcie autoryzacji potwierdzana jest jednak tylko ważność karty oraz wypłacalność posiadacza karty w danej chwili.

Nie można z całą pewnością stwierdzić, czy zamówienie składane jest przez prawowitego posiadacza karty, czy też przez inną osobę bezprawnie posługującą się jego kartą i danymi.

Z tego względu przy zamówieniach składanych faksem lub przez telefon organizacje płatnicze nie przejmują żadnej odpowiedzialności.

Ryzyko spoczywa na Państwa barkach

Oszuści odbierają towar, a prawowici posiadacze kart nie chcą akceptować obciążeń. Dla kontrahenta, której transakcja dotyczy, konsekwencje są często przykre – z jednej strony traci on towar, a z drugiej strony jest zwrotnie obciążany całą kwotą.

Poniższe porady pomogą Państwu ograniczyć ryzyko do minimum:

1. Akceptacja kart

Przyjmowanie zamówień zgodnie z umową o akceptację kart dopuszczalne jest wyłącznie faksem, przez telefon lub sklep internetowy. W przypadku zamówień składanych pocztą elektroniczną z wiadomością zawierającą dane karty należy poinformować nadawcę, że taki sposób zamawiania jest niedopuszczalny.

Przed wysłaniem odpowiedzi należy usunąć numer karty z wiadomości e-mail. Wiadomość drukujemy i usuwamy ją ze „skrzynki odbiorczej” oraz z „kosza”.

2. Dane karty w postaci fizycznej

Dokumentów drukowanych z pełnymi numerami kart nie należy pozostawiać bez nadzoru ani wyrzucać do kosza na śmieci. Takie dokumenty niszczymy w niszczarce do dokumentów, aby nie dało się odtworzyć informacji.

Niepotrzebne dokumenty należy niszczyć na bieżąco.

3. Przekazywanie numerów kart

Przed przekazaniem numerów kart należy zastanowić się, czy odbiorcy faktycznie potrzebny jest cały numer karty. Jeśli nie, numer karty należy przesłać w następującym brzmieniu: XXXX XXXX XXXX 1234. Taki zapis numeru karty nosi miano „PAN truncation”.

Należy bezwzględnie zrezygnować z przesyłania numerów kart w wiadomościach e-mail. Dane karty podajemy przez telefon lub przesyłamy faksem.

4. Zamówienia internetowe

Prowadzącym sklepy internetowe zalecamy korzystanie z nowych zabezpieczeń standardowych „Verified by Visa” i „Mastercard SecureCode” z odpowiednim oprogramowaniem płatniczym (Merchant Plug-In, MPI). Metoda ta pozwala znacznie ograniczyć ryzyko oszustwa.¹

¹Do kart marki Diners Club i Discover oprogramowanie Merchant Plug-In nie jest wymagane.

Dysponując własnym formularzem zamówienia, należy upewnić się, że jest on zgodny ze standardem PCI DSS (bez weryfikacji CVC2/CVV2). Przebieg składania zamówienia należy prześledzić pod kątem przekazywania danych oraz (tymczasowego) zapisywania danych kart, jeśli ma to miejsce.

5. Kontrola zamówienia

Należy zachować ostrożność przy zamówieniach podejrzanie dużych ilości towarów i zamówieniach opiewających na wysokie sumy oraz w przypadku adresów e-mail dostawców bezpłatnych usług, takich jak yahoo.com, gmx.com lub hotmail.com.

6. Kontrola adresu dostawy

Adres dostawy należy skrupulatnie sprawdzić, jeśli różni się on od miejsca zamieszkania zamawiającego.

Kategorycznie odradzamy dostawy towaru do krajów rozwijających się, przede wszystkim do Afryki, na Daleki Wschód oraz do Ameryki Południowej, jak również do państw należących do byłej WNP, jeśli kontrahenci nie są dobrze znani.

Ostrożnie należy podchodzić również do dostaw na adres skrzynek pocztowych lub do hotelu.

7. Ocena ryzyka

Czy byłoby Państwo skłonni do dostarczenia towaru z odroczonym terminem płatności? Karty kredytowe lub debetowe, np. Maestro, to wyjątkowo praktyczny środek płatniczy, który jednak nie pełni funkcji instrumentu windykacji należności.

To Państwo najlepiej wiedzą, w jaki sposób z reguły przebiegają procesy biznesowe w ramach Państwa działalności. Jeśli mają Państwo wątpliwości i jednocześnie chcą dokonać transakcji, zalecamy skontaktować się z własnym bankiem w sprawie gwarancji bankowej.

Osobę do kontaktu w Państwa kraju znaleźć można pod adresem: www.six-payment-services.com/kontakt

SIX Payment Services Ltd
Hardturmstrasse 201
8021 Zurych
Szwajcaria

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luksemburg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Wiedeń
Austria

SIX Payment Services (Germany) GmbH
Langenhorner Chaussee 92-94
22415 Hamburg
Niemcy

