Bezpieczna akceptacja kart

Fałszywe transakcje

Przestrzegaj czterech zasad, aby zachować bezpieczeństwo transakcji:

- **Sprawdź, czy karta jest prawdziwa i bezpieczna.**
- **Zweryfikuj posiadacza karty.**
- **Uważaj na podejrzane zachowanie klienta.**
- **Zaakceptuj transakcję w prawidłowy i bezpieczny sposób.**

Jeśli uważasz, że mogło dojść do oszustwa, zadzwoń do naszego Contact Center i zgłoś „Kod 10”.

801 502 503

Osoby obsługujące terminal mają duży wpływ na wykrywanie i zwalczanie oszustw dokonywanych przy użyciu kart płatniczych. Dlatego należy stosować się do rad spisanych w niniejszym podręczniku i dopilnować, żeby zapoznali się z nim wszyscy pracownicy firmy akceptujący karty. W przypadku jakichkolwiek podejrzeń należy skontaktować się z IT Card Contact Center.

Oto podstawowe zasady bezpieczeństwa:

1. Bądź czujny i nie podejmuj ryzyka.
2. Stosuj się do procedur podanych w podręczniku.
3. Nie przekazuj żadnych poufnych informacji (w tym numeru klienta MID).
4. Nie udostępniaj terminala innym podmiotom.

Jak bezpiecznie akceptować karty?

Sprawdzenie karty

Przed każdą transakcją należy sprawdzić, czy karta ma wszystkie charakterystyczne elementy świadczące o jej oryginalności (rozdział 3.). Należy też zwrócić uwagę na cechy świadczące o tym, że karta może być fałszywa:

- uszkodzenie karty,
- zmiany na pasku do podpisu,
- data ważności niezgodna z datą bieżącą,
- zmiany w obrębie podpisu na karcie,
- brak numeru na pasku do podpisu,
- numer na wydruku z terminala niezgodny z numerem karty,
- zmiany w obrębie numeru karty.

Weryfikacja posiadacza karty

- Jeśli transakcja nie jest weryfikowana przy pomocy numeru PIN, należy sprawdzić, czy podpis złożony na rachunku zgadza się ze wzorem podpisu na karcie.
- Należy porównać numer karty z numerem, który będzie wydrukowany na rachunku (jego całość lub część).
- Jeżeli karta nie jest podpisana, należy poprosić posiadacza karty o złożenie podpisu i jednocześnie o dokument (np. dowód osobisty) w celu zweryfikowania jego tożsamości.
- Należy zwrócić uwagę na zachowanie posiadacza karty (czy zachowuje się swobodnie, czy podejrzanie).

Jeżeli nie jesteś pewien, czy transakcja przeprowadzana jest przez prawowitego posiadacza karty, skontaktuj się z ITCard Contact Center i zastosuj się do instrukcji przekazanych przez operatora.

Podejrzane sytuacje – jak się zachować?

Poza przestrzeganiem wszystkich wymienionych w niniejszym podręczniku procedur należy też obserwować zachowanie posiadacza karty. Twoją uwagę powinny zwrócić tego typu sytuacje:

- kupowanie wielu towarów – bez względu na rozmiary, kolory itp.,
- dokonywanie dużych i częstych zakupów,
- próby odwracania uwagi sprzedawcy od przeprowadzanej transakcji,
- robienie zakupów tuż po otwarciu bądź bezpośrednio przed zamknięciem sklepu.

Oczywiście, podobne zachowanie nie oznacza automatycznie, że ma się do czynienia z oszustem. Najważniejsze to postępować zgodnie ze zdrowym rozsądkiem, oceniając zachowanie posiadacza karty, a w razie jakichkolwiek niejasności, skontaktować się z IT Card Contact Center.

Telefon z „kodem 10”

Telefon pod numer **801 502 503 z „kodem 10”** należy wykonać, gdy:

- posiadacz karty zachowuje się podejrzanie,
- transakcja dokonywana przez posiadacza karty przebiega podejrzanie.

Dzwoniąc, należy:

- mieć przy sobie kartę klienta,
- rozpocząć rozmowę z operatorem od słów: „dzwonię w sprawie autoryzacji, kod 10”,
- spokojnym tonem odpowiadać na wszystkie pytania zadane przez specjalnie przeszkolonego pracownika,
- wykonywać wszelkie polecenia przekazywane przez pracownika IT Card Contact Center,
- powiedzieć posiadaczowi karty, że to rutynowa weryfikacja bezpieczeństwa transakcji,
- podać operatorowi swój unikalny numer klienta TID (znajdziesz go na terminala) oraz podstawowe dane dotyczące transakcji.

Skimming

Skimming to oszustwo polegające na kopiowaniu danych z karty na inną kartę. Na podstawie skradzionych danych produkowane są kolejne karty, które następnie wykorzystywane są przez oszustów.

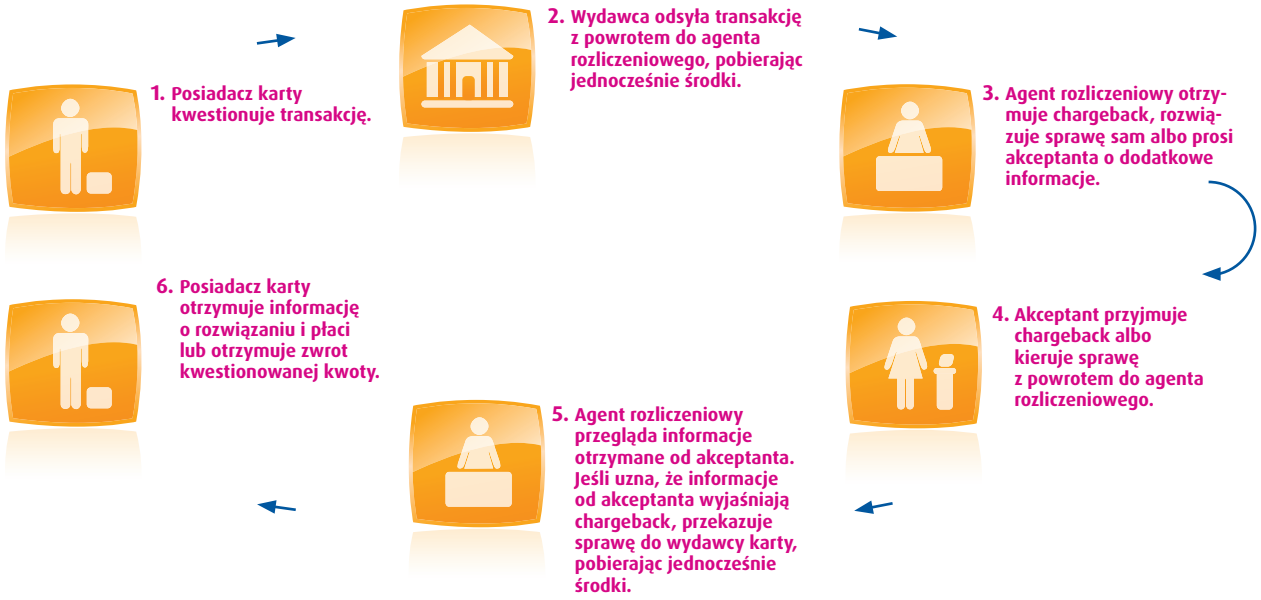
Skimming często zdarza się w miejscach, gdzie posiadacz karty traci ją z oczu, dlatego tak ważne jest przeprowadzanie transakcji w obecności osoby dokonującej płatności kartą.

Reklamacje

8.1 Co to jest chargeback?

Chargeback polega na zwrocie środków z konta akceptanta na konto posiadacza karty, pobranych wcześniej na podstawie pozytywnej autoryzacji transakcji. Powstaje najczęściej w wyniku zareklamowania transakcji przez posiadacza karty.

Poniższy diagram prezentuje poszczególne etapy reklamacji. Umowa z bankiem, który obsługuje transakcje, zawiera szczegółowy opis procedur postępowania w przypadku takiej reklamacji:



Jakie są główne przyczyny powstawania chargebacków?

- **reklamacje klientów**
- **oszustwa**
- **błędy w przeprowadzeniu transakcji**
- **problemy z autoryzacją transakcji**
- **brak odpowiedzi na „żądanie kopii”**

Większości chargebacków można uniknąć, zapewniając pracownikom dobre szkolenie, a także dbając o staranne przeprowadzanie wszystkich transakcji kartami płatniczymi.

Do chargebacku może również dojść w następujących sytuacjach:

- kiedy transakcja zostanie wysłana więcej niż jeden raz (duplikat transakcji),
- posiadacz karty zakwestionuje transakcję,
- transakcja zwrotu zostanie źle przeprowadzona,
- dojdzie do sfałszowania transakcji,
- transakcja zostanie przeprowadzona w imieniu innego podmiotu,
- zostaną naruszone warunki umowy.

Prośba o kopię potwierdzenia transakcji

Zwykle, przed zrobieniem chargebacku, wydawca karty prosi właściciela sklepu lub punktu usługowego o kopię transakcji. Na prośbę banku, we wskazanym terminie, należy dostarczyć dokumenty potwierdzające dokonanie transakcji. W takiej sytuacji trzeba postępować zgodnie ze wskazówkami swojego banku.

Jak unikać reklamacji?

Większość reklamacji spowodowanych jest niedopatrzeniem, ale można ich uniknąć, stosując się do zalecanych procedur.

Warto pamiętać, że:

- Nie należy przeprowadzać transakcji, jeśli otrzymano odmowę autoryzacji. Po otrzymaniu odmowy autoryzacji należy poprosić klienta o inną formę płatności.
- Jeśli transakcja nie jest weryfikowana przy pomocy kodu PIN, należy bardzo dokładnie sprawdzić, czy podpis złożony przez posiadacza karty na rachunku jest zgodny z podpisem na karcie.
- Należy upewnić się, że transakcje zostały wysłane do rozliczenia tylko raz.
- Jeśli transakcja została przeprowadzona w sposób nieprawidłowy lub nie powinna być przeprowadzona, należy pamiętać o jej unieważnieniu.

Zasady bezpiecznego używania Zestawu POS

Zestaw POS to terminal płatniczy oraz inne urządzenia dodatkowe niezbędne do realizacji transakcji takie jak: pin pad, czytnik do kart zbliżeniowych (tzw. contactless), okablowanie zasilające urządzenia oraz okablowanie łączące elementy Zestawu i karta GPRS.

Terminal POS oraz inne niezbędne do realizacji transakcji urządzenia wchodzące w skład zestawu POS przekazane przez Planet Pay nie mogą być podłączone z innym przedmiotem tak, że zestaw POS stałby się jego częścią składową. Nie należy dokonywać zmiany budowy oraz przeznaczenia zestawu POS w tym zmiany stanu technicznego i wyglądu zewnętrznego.

Pamiętaj, aby bezpiecznie akceptować karty zestaw POS musi być zabezpieczony przed utratą czy dostępem do terminala osób nieuprawionych. W przypadku utraty zestawu niezwłocznie poinformuj Planet Pay oraz policję!

Zestaw POS może zostać udostępniony wyłącznie osobie, która jest upoważniona przez Planet Pay, taką osobę (najczęściej będzie to Serwisant) należy wylegitymować oraz zweryfikować jej upoważnienia. Weryfikacja polega na porównaniu kodu przekazanego dla Ciebie przez Planet Pay z kodem otrzymanym od serwisanta.

Uwaga!
Bez pozytywnej weryfikacji nie udostępniaj zestawu POS osobom trzecim.

Inspekcja urządzenia

W celu ochrony przed wyciekiem danych kartowych, należy cykliczne, przynajmniej razna miesiąc, przeprowadzać inspekcje mające na celu weryfikację czy:

- elementy Terminala POS oraz innych urządzeń wykorzystywanych do obsługi transakcji z użyciem kart płatniczych nie noszą znamion manipulacji, np. czy nie zostało zainstalowane lub nie podjęto prób zainstalowania jakiegokolwiek oprogramowania lub urządzenia, które mogłoby służyć do nieuprawnionego rejestrowania lub pozyskiwania danych kart płatniczych lub numerów PIN;
- elementy Terminala POS oraz innych urządzeń wykorzystywanych do obsługi transakcji z użyciem kart płatniczych nie zostały podmienione przez osoby do tego nieuprawnione,
- elementy Terminala POS oraz innych urządzeń wykorzystywanych do obsługi transakcji z użyciem kart płatniczych nie noszą śladów uszkodzeń lub otwierania.

Inspekcja powinna zostać przeprowadzona także w każdym innym momencie wystąpienia podejrzenia ingerencji w elementy Terminala POS oraz innych urządzeń wykorzystywanych do obsługi transakcji z użyciem kart płatniczych.