



OŚWIADCZENIE KLIENTA DOTYCZĄCE REKLAMACJI/ZGŁOSZENIA
NR

OŚWIADCZENIE DOTYCZY:

- NIEAUTORYZOWANEJ TRANSAKCJI PŁATNICZEJ (FRAUDU) – TRANSAKCJE W BANKOWOŚCI INTERNETOWEJ,
- NIEAUTORYZOWANEJ TRANSAKCJI PŁATNICZEJ – TRANSAKCJE KARTOWE,
- REKLAMACJI USŁUGI PŁATNICZEJ,
- REKLAMACJI KARTOWEJ¹.

Imię i nazwisko

.....

Adres

.....

Telefon lub e-mail

.....

Modulo lub PESEL / Regon

.....

Numer rachunku NRB

.....

Numer karty płatniczej*/**.....

Login bankowości internetowej***.....

Kwota reklamowanej transakcji.....

Data transakcji.....

1. Proszę szczegółowo opisać zdarzenie (data, kwota transakcji). Prosimy podać szczegółowo na czym polega Pani/a reklamacja, w jakich okolicznościach i kiedy doszło do reklamowanej usługi płatniczej oraz jakiego działania ze strony Banku Pan/i oczekuje. Prosimy też o załączenie do reklamacji kopii dostępnych dokumentów:

.....
.....
.....

2. Proszę określić sposób, w jaki oszuci nawiązali z Panem/ią kontakt?:

- link,
- SMS,
- e-mail,
- połączenie telefoniczne,

¹ Niepotrzebne skreślić

inny (podać jaki?)

3. W jaki sposób zostały wykonane reklamowane transakcje?:

- portfel Google Pay (portfel Google),
- portfel Apple Pay (Apple Wallet),
- transakcje na stronie internetowej,
- transakcje z użyciem kodu BLIK,
- przelewem tradycyjnym (placówka Banku),
- aplikacja mobilna (telefon),
- bankowości elektroniczna (komputer),

inny (jaki?).....
 nie wiem.

4. Czy zna Pan/i zasady bezpiecznego korzystania z urządzeń komputera, telefonu i bankowości internetowej?

TAK/NIE

5. Czy posiada Pan/i program antywirusowy na swoim urządzeniu?

TAK/NIE

6. Czy z Pana/i komputera/telefonu korzysta inna osoba?

TAK/NIE

7. Czy strona internetowa eBankNet/ eCorpoNet wyglądała inaczej niż zazwyczaj?***

TAK/NIE

Jeśli TAK proszę opisać wygląd strony

.....

8. Czy w ostatnim czasie zauważył/a Pan/i nietypowe lub podejrzane zdarzenia związane z działaniem telefonu, komputera, bankomatu czy karty płatniczej (za zdarzenie nietypowe / podejrzane należy uznać m.in.: otrzymanie nieoczekiwanego e-maila z fakturą lub linkiem, otrzymanie e-maila z treścią napisaną w języku obcym, z błędami, od nieznanego nadawcy, otrzymanie sms poprzez Messenger/WhatsApp od kolegi potrzebującego szybkiej pożyczki, nieprawidłowe działanie urządzenia, zgubienie karty płatniczej)?

TAK/NIE

Jeśli TAK proszę podać szczegóły.

.....

.....

.....

9. Czy w dniu zdarzenia dokonywał/a Pan/i zakupów poprzez portale zakupowe np. OLX, Vinted lub dzwoniła do Pana/i osoba podająca się za maklera, brokera lub pracownika banku lub innej instytucji zaufania publicznego(policja, prokuratura, służby specjalne)?

TAK/NIE

Jeśli TAK proszę podać szczegóły.

.....

.....

10. Czy dane odnośnie loginu i hasła do systemu eBankNet/ eCorpoNet lub kod BLIK został/y podane/y np. innej osobie np. w rozmowie telefonicznej lub na stronie internetowej?***

TAK/NIE

Jeśli TAK proszę o podanie szczegółów np. numer telefonu z jakiego zostało wykonane połączenie lub adres strony internetowej.

.....

.....

11. Czy podał/a Pan/i innej osobie kod uwierzytelniający PIN do transakcji internetowych (ustawiany przez klienta w portalu kartowym Kartosfera) albo kod 3D Secure otrzymany z Banku?

TAK/NIE

12. Na jaki numer telefonu otrzymał/a Pan/i sms od Banku w dniu zdarzenia? Prośba o ich pokazanie lub jeśli to możliwe o przesłanie na skrzynkę email pracownika prowadzącego sprawę np. zdjęcia lub zrzutu ekranu?:

.....

13. Czy podczas wpisywania kodów z sms zapoznał/a się Pan/i z ich treścią?

TAK/NIE

14. Czy Pan/i autoryzował/a samodzielnie kwestionowane transakcje?

TAK/NIE

15. Czy podejrzewa Pan/i kto mógł dokonać transakcji z Pana/i rachunku?***

TAK/NIE

Jeśli TAK proszę podać szczegóły.

.....
16. Czy dokonał/a Pan/i zawiadomienia na policję/prokuraturę o podejrzeniu popełnienia przestępstwa?:

TAK/NIE

Jeśli TAK proszę o podanie jednostki policji/prokuratury, do której zostało dokonane zawiadomienie lub okazanie/przesłanie zaświadczenia o złożonym zawiadomieniu.

17. Jeśli NIE czy zamierza Pan/Pani takiego zawiadomienia dokonać?:

TAK/NIE

18. Dołączam wydane przez Policję potwierdzenie o dokonaniu zgłoszenia na Policji dokonania nieautoryzowanych transakcji:***

TAK NIE

19. Czy dane odnośnie loginu i hasła do portalu kartowego Kartosfery, karty płatniczej/kredytowej (numer karty, data ważności, kod CVV, kod PIN do transakcji internetowych lub kod BLIK został/y podany/e innej osobie np. w rozmowie telefonicznej lub na stronie internetowej?***

TAK/NIE

Jeśli TAK proszę o podanie szczegółów np. numer telefonu z jakiego zostało wykonane połączenie lub adres strony internetowej.

20. Czy w okresie 14 dni przed dokonaniem transakcji, przekazywałam/em informacje dotyczące rachunku, danych logowania lub danych karty, poprzez:

- WhatsApp
- Viber
- Messenger
- link w przesyłce e-mail
- formularz na stronie www
- rozmowa telefoniczna (z jakiego numeru)
- inny
- nie

21. Czy w okresie 14 dni od reklamowanej transakcji dokonywał/a Pan/i transakcji kupna lub sprzedaży z wykorzystaniem portali ogłoszeniowych np. OLX, Allegro, Vinted lub innych?

- OLX
- Vinted
- Allegro
- Allegro lokalnie
- inne
- nie

22. Czy w okresie 14 dni od reklamowanej transakcji, przekazał/a Pan/i na prośbę wystosowaną za pośrednictwem poczty elektronicznej, wiadomości SMS, komunikatora (np. WhatsApp, Viber, Messenger) lub w innych sposób, któreś z poniższych danych?:

- Identyfikator (login) i/lub hasło do bankowości internetowej
- Kod E- PIN (numer identyfikujący użytkownika korzystającego z aplikacji mobilnej)
- Kod SMS (hasło przesyłane na telefon do autoryzacji transakcji lub innych dyspozycji)
- Kod silnego uwierzytelnienia
- Inne dane: proszę podać jakie?
- Nie, nie podawałam żadnych z w/w danych.

Do reklamacji należy załączyć fotokopii/skany tej korespondencji.

Co zawierała korespondencja z osobą, która się kontaktowała:

.....
.....

Czy podano adres strony na który należało wejść (link do strony)?:

.....

.....
Czy przesłano wiadomość e-mail z dalszymi instrukcjami (co były w treści maila)?:
.....
.....
.....
.....

Jakie dane zostały podane?:

- numer karty
- data ważności
- kod CVC/CVV
- PIN
- kod 3D Secure

23. Czy w okresie 14 dni od reklamowanej transakcji, przychodziły do Pana/i kody SMS, których używał/a Pan/i do autoryzacji?

- Tak
- Nie

W przypadku odpowiedzi „Tak”, proszę załączyć fotokopie/skany/screeny treści tych wiadomości.

24. Czy w okresie 14 dni od reklamowanej transakcji wchodził Pan/i na strony internetowe za pośrednictwem linków (odsyłających do strony) przesłanych za pośrednictwem poczty elektronicznej, wiadomości SMS, komunikatora (np. WhatsApp, Viber, Messenger) lub w innych sposób?:

- Tak
- Nie

W przypadku odpowiedzi „Tak”, proszę załączyć fotokopie/skany/screeny treści tej korespondencji.

25. Czy w okresie 14 dni od reklamowanej transakcji kierowano do Pani/a za pośrednictwem poczty elektronicznej, wiadomości SMS, komunikatora (np. WhatsApp, Viber, Messenger) lub w innych sposób prośbę o zainstalowanie dodatkowego oprogramowania – i czy dokonał/a Pan/i instalacji takiego oprogramowania?***

- Nie

Tak, jakiego ? (np. TeamViewer, Quick Support, AnyDesk, inne).....

Do reklamacji należy załączyć fotokopii/skany tej korespondencji

Oświadczam, że:

Nie dokonałem/am reklamowanych transakcji ani nie upoważniałem nikogo do ich dokonania.

26. Upoważniam do zablokowania wszelkich kanałów dostępu do narzędzi umożliwiających dokonywanie transakcji w ciężar mojego rachunku [blokada karty płatniczej, blokada aplikacji mobilnej, blokada aplikacji BLIK], z wyłączeniem blokady samego rachunku bankowego]***

27. Upoważniam Bank Spółdzielczy w Jordanowie do udostępnienia moich danych osobowych i danych objętych tajemnicą bankową organom ścigania na potrzeby prowadzenia postępowania wyjaśniającego i będących w związku z złożoną reklamacją***

- TAK NIE

Data.....

Podpis Posiadacza rachunku.....

Kopię przyjętego zgłoszenia przekazano klientowi

- TAK
 - NIE - podać przyczyny:
-
.....

* dotyczy zgłoszenia nieautoryzowanej transakcji płatniczej (fraud) - transakcje kartowe,

** dotyczy zgłoszenia reklamacji kartowej,

*** dotyczy zgłoszenia nieautoryzowanej transakcji płatniczej
