NIEAUTORYZOWANE TRANSAKCJE, PROBLEMY PRAKTYCZNE – CZY ZMIANY PO WEJŚCIU PSR JE ROZWIĄŻĄ ?

KANCELARIE RADCÓW PRAWNY

ANETA CIECHOWICZ-JAWORSKA, BARTŁOMIEJ ŚLAŻYŃSKI

DEFINICJA USTAWOWA AUTORYZOWANEJ TRANSAKCJI PŁATNICZEJ

Zgodnie z art. 40 ust. 1 ustawy o usługach płatniczych:

„Transakcję płatniczą uznaje się za autoryzowaną wyłącznie wówczas, gdy płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a dostawcą."

TRANSAKCJA AUTORYZOWANA = TRANSAKCJA NA, KTÓRĄ PŁATNIK WYRAZIŁ ZGODĘ

POJĘCIE TRANSAKCJI NIEAUTORYZOWANEJ *A CONTRARIO*

- Przez nieautoryzowaną transakcję płatniczą należy rozumieć transakcję wykonaną bez zgody płatnika albo z przekroczeniem zakresu udzielonej przez niego zgody.
- Dla uznania transakcji za autoryzowaną konieczne jest świadome i skuteczne wyrażenie przez płatnika zgody na jej wykonanie w sposób przewidziany w umowie zawartej z dostawcą usług płatniczych.
- Brak takiej zgody skutkuje kwalifikacją transakcji jako nieautoryzowanej.

WYRAŻENIE WOLI KLIENTA A AUTORYZACJA TRANSAKCJI 1/2

- Autoryzacja transakcji wymaga **świadomego i jednoznacznego wyrażenia zgody przez płatnika**.
- Zgoda musi obejmować **konkretną transakcję**, jej odbiorcę, kwotę oraz cel płatności.
- Transakcja nie powinna być uznawana za autoryzowaną jeżeli została zainicjowana lub modyfikowana przez podmiot trzeci, który **działał bez zgody użytkownika,** w tym używając **danych uwierzytelniających użytkownika, pozyskanych w sposób oszukańczy.**
- Samo użycie danych uwierzytelniających (PIN, kod SMS, autoryzacja w aplikacji) nie zawsze oznacza skuteczne wyrażenie woli przez klienta.

WYRAŻENIE WOLI KLIENTA A AUTORYZACJA TRANSAKCJI 2/2

- W przypadku oszustw typu **phishing, vishing lub spoofing** klient może dokonać technicznej autoryzacji, pozostając w błędnym przekonaniu co do rzeczywistego charakteru transakcji.
- Istotne jest rozróżnienie pomiędzy:
  - **technicznym uwierzytelnieniem transakcji**, a
  - **rzeczywistą zgodą klienta na wykonanie płatności**.
- Brak świadomej zgody płatnika może prowadzić do uznania transakcji za **nieautoryzowaną**.

UWAGA: Ciężar dowodu poprawnie przeprowadzonej autoryzacji spoczywa na dostawcy usług płatniczych.

WYROK SĄDU NAJWYŻSZEGO - IZBA CYWILNA Z DNIA 15 WRZEŚNIA 2023 R. II CSKP 1013/22

O ile autoryzacja to zgoda na wykonanie transakcji płatniczej wyrażona przez płatnika w sposób przewidziany w umowie, o tyle uwierzytelnienie to procedura umożliwiająca dostawcy usług (bankowi) na weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika.

Samo podanie danych umożliwiających zalogowanie do bankowości elektronicznej, w sytuacji gdy dla autoryzacji (potwierdzenia) czynności potrzebne jest jeszcze podanie kodów autoryzacyjnych przesłanych w treści wiadomości SMS, nie stanowi jeszcze przejawu rażącego niedbalstwa. Dopiero udostępnienie danych logowania oraz kodów autoryzacyjnych może być poczytywane jako przejaw rażącego niedbalstwa, szczególnie wówczas gdy z treści wiadomości SMS wynika, że kod służy autoryzacji czynności, której uprawniony użytkownik nie zamierza autoryzować, innymi słowy nie zamierza jej przeprowadzić.

Wykazanie uwierzytelnienia transakcji płatniczej nie jest równoznaczne z wykazaniem jej autoryzacji.

WYROK SĄDU APELACYJNEGO W KRAKOWIE - I WYDZIAŁ CYWILNY Z DNIA 19 KWIETNIA 2023 R. I AGA 292/21

Zgodnie z art. 40 ustawy o usługach płatniczych transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zgoda ta może być wyrażona pośrednio także poprzez upoważnienie innej osoby do dokonywania transakcji poprzez dodanie jej jako odbiorcy zaufanego. Ciężar udowodnienia tych okoliczności spoczywa jednak na dostawcy. W przeciwnym razie transakcja nie może być uznana za autoryzowaną.

CZAS OBECNIE NA PSR

PSR

- Komisja Europejska uznała, że wdrożenie PSD2 przez państwa członkowskie doprowadziło do znacznych różnic w stosowaniu przepisów, rozbieżności interpretacyjnych oraz nierównego poziomu ochrony użytkowników usług płatniczych w poszczególnych krajach UE.
- W związku z tym zdecydowano o przyjęciu **Payment Services Regulation (PSR)** jako rozporządzenia obowiązującego bezpośrednio we wszystkich państwach członkowskich.

PSR

- **PSR (Payment Services Regulation)** to projektowane rozporządzenie Unii Europejskiej, które ma zastąpić część obecnych regulacji wynikających z Dyrektywy PSD2 i stworzyć jednolite zasady świadczenia usług płatniczych we wszystkich państwach członkowskich UE.
- W przeciwieństwie do dyrektywy, która wymaga implementacji do prawa krajowego, rozporządzenie będzie stosowane bezpośrednio we wszystkich państwach członkowskich, bez konieczności uchwalania odrębnych przepisów krajowych.

GŁÓWNE CELE WPROWADZENIA PSR

- **Ujednolicenie zasad świadczenia usług płatniczych w całej Unii Europejskiej.**
- **Eliminacja rozbieżności wynikających z krajowych implementacji PSD2.**
- **Wzmocnienie ochrony konsumentów przed nowoczesnymi formami oszustw płatniczych**, w szczególności phishingiem, spoofingiem i oszustwami polegającymi na podszywaniu się pod bank.
- **Zwiększenie bezpieczeństwa transakcji płatniczych i ograniczenie skali fraudów.**
- **Zapewnienie większej pewności prawa dla dostawców usług płatniczych działających transgranicznie.**
- **Ułatwienie działalności fintechów i innych podmiotów działających na rynku płatności.**
- **Wprowadzenie jednolitych standardów bezpieczeństwa oraz przeciwdziałania oszustwom na poziomie całej UE.**
- **Usprawnienie nadzoru i egzekwowania przepisów poprzez stosowanie jednolitych regulacji we wszystkich państwach członkowskich.**

NAJWAŻNIEJSZA ZMIANA REGULACYJNA

- **PSD2 ustanawiała wspólne zasady, ale ich stosowanie zależało od sposobu implementacji do prawa krajowego.**
- **PSR tworzy jednolity zbiór przepisów obowiązujących bezpośrednio w całej Unii Europejskiej, co ma zapewnić większą spójność regulacyjną, wyższy poziom ochrony klientów oraz skuteczniejsze przeciwdziałanie oszustwom.**

KLUCZOWE FILARY ZMIAN NA GRUNCIE PSR

ODPOWIEDZIALNOŚĆ DOSTAWCY USŁUG PŁATNICZYCH ZA TRANSAKCJE NIEAUTORYZOWANE

ODPOWIEDZIALNĆ DOSTAWCY USŁUG PŁATNICZYCH ZA OSZUKAŃCZE TRANSAKCJE PŁATNICZE – *SPOOFING*

USŁUGA WERYFIKACJI DOPASOWANIA ODBIORCY

NIEAUTORYZOWANE TRANSAKCJE – USTAWA O USŁUGACH PŁATNICZYCH (PSD2) VS PSR

Obszar	Obecny stan prawny (UUP / PSD2)	PSR (projekt)
Definicja autoryzacji	Klient musi wyrazić zgodę na wykonanie transakcji.	Bez zmian – kluczowe pozostaje wyrażenie zgody przez płatnika.
Punkt ciężkości analizy	Czy klient autoryzował transakcję?	Czy klient autoryzował transakcję oraz czy PSP skutecznie zapobiegał oszustwu?
Nieautoryzowana transakcja	Brak zgody klienta = obowiązek zwrotu środków przez PSP.	Zasada utrzymana.
Spoofing / phishing / impersonation fraud	Brak odrębnych regulacji dla nowych modeli oszustw.	Wyraźne uwzględnienie oszustw opartych na podszywaniu się pod bank lub instytucję płatniczą.
Ciężar dowodu	PSP wykazuje uwierzytelnienie, rejestrację transakcji i brak awarii systemu.	Utrzymany, ale rozszerzony o obowiązki wykazania skutecznych mechanizmów antyfraudowych.
Zwrot środków klientowi	Niezwłoczny zwrot po stwierdzeniu nieautoryzowanej transakcji.	Zasada pozostaje bez zmian.
Monitoring fraudów	Ograniczone obowiązki ustawowe.	Znacznie szersze obowiązki monitorowania i wykrywania oszustw.
Weryfikacja odbiorcy płatności	Brak pełnego obowiązku weryfikacji nazwy odbiorcy i IBAN.	Obowiązkowy mechanizm Verification of Payee (VoP).
Wymiana informacji o oszustwach	Ograniczona.	Szersza możliwość i obowiązek wymiany danych o fraudach pomiędzy PSP.
Odpowiedzialność PSP	Skoncentrowana na autoryzacji transakcji.	Większa odpowiedzialność za niewdrożenie odpowiednich środków bezpieczeństwa.

PSD2 koncentruje się głównie na zachowaniu klienta i jego zgodzie na transakcję. PSR przesuwa część odpowiedzialności na dostawców usług płatniczych, wymagając aktywnego zapobiegania oszustwom i wdrożenia zaawansowanych mechanizmów antyfraudowych.

ODPOWIEDZIALNOŚĆ DOSTAWCY USŁUG PŁATNICZYCH ZA TRANSAKCJE NIEAUTORYZOWANE 1/2

- PSP DOKONUJE ZWROTU W TERMINIE D+1, OD ZGŁOSZENIA ZDARZENIA PRZEZ PŁATNIKA LUB ODNOTOWANIA NTP, NA KONCIE KLIENTA
- MOŻLIWA ODMOWA ZWROTU PRZEZ PSP JEŻELI PŁATNIK WYKAZAŁ SIĘ RAŻĄCYM NIEDBALSTWEM. PSP POWIADAMIA KLIENTA NA PIŚMIE O ODMOWIE ZWROTU
- BRAK ZWROTU Z UWAGI NA PODEJRZENIE OSZUKAŃCZEGO DZIAŁANIA PŁATNIKA – PSP PRZEKAZUJE ZAWIADOMIENIE DO ODPOWIEDZNIEGO ORGANU

ODPOWIEDZIALNOŚĆ DOSTAWCY USŁUG PŁATNICZYCH ZA TRANSAKCJE NIEAUTORYZOWANE 2/2

- PRAWIDŁOWE ZGŁOSZENIE NTP PRZEZ PŁATNIKA, BEZ ZBĘDNEJ ZWŁOKI I Z ZACHOWANIEM TERMINU 18 MSC. = OBOWIĄZEK ZWROTU TRANSAKCJI NIEAUTORYZOWANEJ PRZEZ PSP. WYJĄTEK ART. 60 PSR.
- ZWROT RÓWNOWARTOŚCI TRANSAKCJI NIEAUTORYZOWANEJ = PRZYWRÓCENIE RACHUNKU DO STANU JAKI ISTNIAŁBY GDYBY NIE DOSZŁO DO PŁATNOŚCI NIEAUTORYZOWANEGO.
- PODEJRZENIE POPEŁNIENIA OSZUSTWA/RAŻĄCE NIEDBALSTWO W ZWIĄZKU Z TRANSAKCJĄ NIEAUTORYZOWANĄ PRZEZ PŁATNIKA = PRZEPROWADZENIE POSTĘPOWANIA WYJAŚNIAJĄCEGO I EWENTUALNA ODMOWA.
- DODATKOWO PŁATNIKOWI, POZA ZWROTEM RÓWNOWARTOŚCI NTP, NA PODSTAWIE ODRĘBNYCH PRZEPISÓW MOGĄ PRZYSŁUGIWAĆ REKOMPENSATY FINANSOWE.

TRANSAKCJE NIEAUTORYZOWANE – POSTĘPOWANIE WYJAŚNIAJĄCE 1/3

UWAGA ! W PRZYPADKU UZNANIA, ŻE DO TRANSAKCJI NIEAUTORYZOWANEJ DOSZŁO W ZWIĄZKU Z OSZUSTWEM PŁATNIKA LUB WYKAZANIEM SIĘ PRZEZ NIEGO RAŻĄCYM NIEDBALSTWEM, PSP WINIEN ZAPROSIĆ PŁATNIKA DO WYJAŚNIENIA OKOLICZNOŚCI ZWIĄZANYCH Z TRANSAKCJĄ NIEAUTORYZOWANĄ.

TRANSAKCJE NIEAUTORYZOWANE – POSTĘPOWANIE WYJAŚNIAJĄCE 2/3

- TERMIN NA WYDANIE DECYZJI PRZEZ PSP W RAMACH POSTEPOWANIA WYJAŚNIAJĄCEGO WYNOSI 15 DNI
- W PRZYPADKU WYDANIA DECYZJI ODMOWNEJ, PSP MA OBOWIĄZEK WSKAZAĆ PŁATNIKOWI ORGANY, DO KTÓRYCH BĘDZIE MÓGŁ SIĘ ODWOŁAĆ
- PSP PO PRZEPROWADZENIU POSTĘPOWANIA WYJASNIAJĄCEGO MOŻE PODJĄĆ DECYZJĘ O ZWROCIE ŚRODKÓW

TRANSAKCJE NIEAUTORYZOWANE – POSTĘPOWANIE WYJAŚNIAJĄCE 3/3

PSD2/UUP

- zasada: "refund first, investigate later"

PSR

- możliwość odmowy natychmiastowego zwrotu przy istnieniu obiektywnie uzasadnionych podstaw do podejrzenia oszustwa lub rażącego niedbalstwa klienta,
- obowiązek przedstawienia klientowi pisemnego uzasadnienia i informacji o środkach odwoławczych w terminie 15 dni roboczych.
- Jednocześnie warto podkreślić, że **samo podejrzenie nie wystarczy**. PSR posługuje się pojęciem *objectively justified grounds* (obiektywnie uzasadnione podstawy), co oznacza, że bank będzie musiał wykazać konkretne okoliczności uzasadniające odmowę zwrotu. To prawdopodobnie stanie się przedmiotem licznych sporów po wejściu PSR w życie.

ODPOWIEDZIALNOŚĆ DOSTAWCY USŁUG PŁATNICZYCH ZA OSZUKAŃCZE TRANSAKCJE PŁATNICZE – SPOOFING 1/2

- *SPOOFING* – oszustwo polegające na podszywaniu się przez przestępców pod różnego rodzaju instytucje, w tym banki, celem zdobycia zaufania klientów tych instytucji, a następnie wyłudzenia danych, pieniędzy lub zainfekowania urządzeń złośliwym oprogramowaniem. Oszuści posługują się przy tym numerami telefonów lub adresami mailowymi, należących do instytucji pod które się podszywają.
- Charakterystyczne dla tego typu oszustwa, jest to, że **płatnik faktycznie dokonuje autoryzacji transakcji samodzielnie, ale czyni to pod wpływem błędnego przekonania, co do tożsamości podmiotu, z którym się komunikuje.**
- Regulacje dotyczące spoofingu znajdują zastosowanie wyłącznie, wobec użytkowników posiadających **status konsumenta.**

ODPOWIEDZIALNOŚĆ DOSTAWCY USŁUG PŁATNICZYCH ZA OSZUKAŃCZE TRANSAKCJE PŁATNICZE – SPOOFING 2/2

- PSP ZOBOWIĄZANY DO BLOKOWANIA OSZUSTOM MOŻLIWOŚCI PODSZYWANIA SIĘ POD KANAŁY KOMUNIKACJI Z UŻYTKOWNIKIEM.
- PSP ZOBOWIĄZANY DO WPROWADZENIA ODPOWIEDNICH ZABEZPIECZEŃ TECHNICZNYCH, MAJĄCYCH NA CELU OCHRONĘ PRZED METODAMI DZIAŁAŃ STOSOWANYCH PRZEZ OSZUSTÓW.
- PSP ZWRACA KLIENTOWI UTRACONA KWOTĘ W TERMINIE 15 DNI ROBOCZYCH OD ZGŁOSZENIA TRANSAKCJI OSZUKAŃCZEJ. ZWROT WYMAGA RAPORTU POLICJI POTWIERDZAJĄCEG ZGŁOSZENIE PRZESTĘPSTWA ORGANOM ŚCIGANIA.
- OBOWIĄZEK WYSŁUCHANIA UŻYTKOWNIKA PRZEZ PSP PRZED PODJĘCIEM DECYZJI.

USŁUGA WERYFIKACJI DOPASOWANIA ODBIORCY

Przy zlecaniu przelewu płatnik określa dane odbiorcy w tym jego dane i unikatowy identyfikator

Dostawca płatnika inicjuje weryfikację danych odbiorcy u dostawcy odbiorcy

Ewentualne rozbieżności w danych odbiorcy są komunikowane płatnikowi

Akceptacja rozbieżności przez płatnika wyłącza wadliwość transakcji

USŁUGA WERYFIKACJI DOPASOWANIA ODBIORCY PRZYKŁAD PRAKTYCZNY

Przykład:

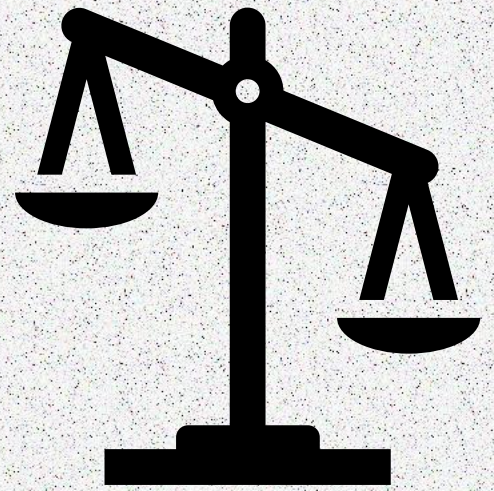
- Klient chce przelać 50 000 zł na rachunek wskazany przez „pracownika banku”.
- System wyświetla komunikat:
- „Nazwa odbiorcy nie odpowiada właścicielowi rachunku.”

Klient mimo tego:

- ignoruje ostrzeżenie,
- potwierdza przelew,
- pieniądze trafiają do oszusta.

W takim przypadku bank będzie miał znacznie silniejszy argument, że klient świadomie zignorował ostrzeżenie bezpieczeństwa.

CO GDY NIEAUTORYZOWANA TRANSAKCJA STAJE SIĘ PRZEDMIOTEM SPORU MIĘDZY BANKIEM A KLIENTEM ?



NTP PROBLEM OBECNY

Bank często wskazuje, że:

- klient użył prawidłowych danych uwierzytelniających w tym prawidłowego loginu, hasła, PIN-u lub autoryzacji mobilnej;
- klient samodzielnie zatwierdził transakcję kodem SMS lub w aplikacji;
- klient udostępnił dane uwierzytelniające lub instrument płatniczy nieznanym osobom trzecim;
- klient nie zważał na komunikaty informacyjne banku dotyczące cyberbezpieczeństwa;
- klient wykazał się rażącym niedbalstwem i nie dopełnił obowiązków spoczywających na nim w ramach umowy ramowej i UUP;
- po stronie banku nie nastąpiła żadna awaria techniczna ani systemowa oraz nie doszło do przełamania zabezpieczeń banku;
- nie nastąpiło żadne włamanie hakerskie do systemów bankowych;
- bank spełnił obowiązek uwierzytelnienia klienta (SCA)

NTP PROBLEM OBECNY

Klient twierdzi natomiast, że:

- został oszukany/zmanipulowany (phishing, spoofing, vishing i.in.);
- nie wiedział, co autoryzuje;
- nie autoryzował transakcji w sposób świadomy;
- przestępca przejął kontrolę nad urządzeniem;
- bank niedostatecznie zabezpieczył środki na koncie klienta,
- bank nie zastosował stosownych blokad, zabezpieczeń i systemów
- samo wykazanie poprawnego uwierzytelnienia nie oznacza jeszcze, że transakcja była prawidłowo autoryzowana przez klienta.

CO POZOSTAJE BEZ ZMIAN PO STRONIE PŁATNIKA ?

Na gruncie PSR klient nadal będzie odpowiadał za:

- umyślne działanie;
- rażące niedbalstwo;
- ignorowanie wyraźnych ostrzeżeń bezpieczeństwa;
- brak poinformowania o ntp niezwłocznie, nie później niż w terminie 18 mec. od dnia wykonania transakcji (jedyna zmiana terminu zgłoszenia z 13 msc. Na 18 msc.);
- odpowiedzialność użytkownika do 50 EUR lub pełna odpowiedzialność — zależnie od tego, czy po stronie płatnika wystąpiły nieuczciwe zamiary, rażące niedbalstwo lub użycie utraconego, skradzionego czy przywłaszczonego instrumentu albo danych uwierzytelniających;
- niewłaściwe zabezpieczenie danych uwierzytelniających.

CZY PSR ROZWIĄŻE TEN SPÓR?

- PSD2 koncentruje się głównie na zachowaniu klienta i jego zgodzie na transakcję. PSR przesuwa część odpowiedzialności na dostawców usług płatniczych, wymagając aktywnego zapobiegania oszustwom i wdrożenia zaawansowanych mechanizmów antyfraudowych.
- PSR nie zmienia definicji nieautoryzowanej transakcji, ale znacząco podnosi standard należytej staranności wymaganej od banków i instytucji płatniczych.
- PSR nie zmienia zasad odpowiedzialności klienta za umyślne działanie lub rażące niedbalstwo, ale znacząco zwiększa odpowiedzialność dostawców usług płatniczych za zapobieganie oszustwom oraz wykrywanie podejrzanych transakcji. **W praktyce więcej sporów będzie dotyczyć jakości systemów bezpieczeństwa banku, a nie wyłącznie zachowania klienta.**

CO ZMIENI SIĘ W PRAKTYCE ?

- Odpowiedzialność za sam fakt oszustwa będzie w większym stopniu oceniana także przez pryzmat działań banku. W praktyce oznacza to, że po wejściu PSR **kluczowe pytanie nie będzie już brzmiało wyłącznie „co zrobił klient?", ale również „co zrobił bank, aby temu oszustwu zapobiec?";**
- Rozdzielenie autoryzacji i uwierzytelnienia utrudni wykazywanie prawidłowej autoryzacji transakcji;
- Utrzymanie ciężaru dowodu po stronie banku zwiększy ryzyko sporów dotyczących transakcji nieautoryzowanych;
- Wykazanie świadomej woli płatnika będzie w praktyce znacząco utrudnione (banki nie dysponują narzędziami pozwalającymi na obiektywna ocenę świadomości użytkownika w chwili zlecenia transakcji);
- Postępowania wyjaśniające = wdrożenie nowych procedur wewnątrzbankowych, czasochłonne i bardziej złożone postepowania reklamacyjne, zwrost kosztów i obciążeń operacyjnych po stronie bank;
- Zakres odpowiedzialności dowodowej banków, może wykraczać poza ich techniczną rolę w realizacji transakcji płatniczych.

KANCELARIA RADCÓW PRAWNYCH
ANETA CIECHOWICZ-JAWORSKA
BARTŁOMIEJ ŚLAŻYŃSKI

ul. Wilcza 31 lok 10A, 00-544 Warszawa

Phone/fax: 0048 22 628 22 02

www.radca-warszawa.com.pl