BARBARA BAJOR

Problematyka nieautoryzowanych transakcji płatniczych – wybrane aspekty prawne

The Problem of Unauthorized Payment Transactions – Selected Legal Aspects

Abstract

With the rise of electronic payment transactions, the issue of unauthorized payment transactions has become extremely important, both from the perspective of the party affected by the financial consequences of such transactions and in terms of determining who bears responsibility for unauthorized payment transactions. Clarifying the meaning of the term "unauthorized transactions" – which, it would seem, should not raise any doubts – is, however, a problematic issue in practice.

SŁOWA KLUCZOWE: autoryzacja, uwierzytelnianie, transakcja płatnicza, nieautoryzowane transakcje płatnicze.

KEY WORDS: authorization, authentication, payment transaction, unauthorized payment transactions.

BARBARA BAJOR – doktor habilitowany nauk prawnych, profesor Europejskiej Wyższej Szkoły Prawa i Administracji w Warszawie, e-mail: bbajor@ewspa.edu.pl, ORCID – 0000-0002-1647-3297.

1 Uwagi wprowadzające

Istota problemu polega na precyzyjnym ustaleniu zakresu pojęciowego „nieautoryzowane transakcje płatnicze". Na tym tle, mimo wydawałoby się jasnego sformułowania, powstaje szereg nieścisłości. Stan ten nie sprzyja jasności i z całą pewnością pozwala na różne ujęcia tej kwestii. W konsekwencji ma też decydujące znaczenie dla ustalenia zakresu odpowiedzialności i podmiotu odpowiedzialnego[1]. Powyższe rozbieżności związane są z trudnościami w

1 „Prawidłowa, zgodna z określonymi w załączonych do umowy ramowej regulaminami, autoryzacja jest zasadniczym elementem w procesie przeprowadzania transakcji. Przede wszystkim od ustalenia, czy doszło do autoryzacji transakcji płatniczej przez użytkownika, czy też mamy do czynienia z transakcją nieautoryzowaną, zależy odpowiedzialność zarówno dostawcy, jak i płatnika za transakcję płatniczą. Natomiast

HTTPS://DOI.ORG/10.36128/FKXTE318

precyzyjnym, a przede wszystkim jednolitym ustaleniu również znaczeń pojęć „autoryzacja" i „uwierzytelnianie". Zwraca się bowiem uwagę w literaturze, że polski ustawodawca mylnie przetłumaczył postanowienia pierwszej dyrektywy PSD[2], a następnie nie skorygował błędu w trakcie wdrożenia postanowień dyrektywy PSD2[3].

Zapewne należałoby również zastanowić się, czym jest uwierzytelnianie, a czym autoryzacja i w konsekwencji kiedy mamy do czynienia z nieautoryzowanymi transakcjami. Czy słusznie należałoby przyjąć – zgodnie z literalnym brzmieniem tego sformułowania – że są to tylko te transakcje, które nie zostały autoryzowane?

Przy czym niezależnie od uznania, czy doszło do błędnego przetłumaczenia tekstu dyrektywy, od 2011 r. obowiązują określone rozwiązania (wraz z dość istotną zmianą przepisów ustawy w 2018 r.[4] w związku z przyjęciem dyrektywy PSD2) i na ich podstawie ocenia się, czy doszło do nieautoryzowanych transakcji. Stąd różne poglądy, które służą wyjaśnieniu i doprecyzowaniu. Należy przy tym mieć również na uwadze zmiany, które nastąpią w związku

od ustalenia, z jakich przyczyn doszło do wykonania nieautoryzowanej przez płatnika transakcji, zależy zakres odpowiedzialności dostawcy i obowiązku zwrotu kwot nieautoryzowanych transakcji" – wyrok Sądu Okręgowego w Krakowie z dnia 3 lipca 2018 r., II Ca 452/18, LEX nr 2780921.

2 Jak podkreślają Marcin Blocher, Wojciech Iwański, „Nieautoryzowane transakcje płatnicze" *Monitor Prawniczy*, nr 9 (2020): 465–471: „Do niedawna pojęcie «uwierzytelnianie» nie było używane na gruncie UsłPłU, pomimo że zostało wprowadzone w ramach PSD1. Prawodawca europejski – zarówno na gruncie PSD1, jak i PSD2 – ściśle rozróżnia pojęcie «autoryzacji» i «uwierzytelniania». Historycznie, w wyniku oczywistej pomyłki rozróżnienie to nie znalazło odzwierciedlenia w polskim tłumaczeniu dyrektywy PSD1. Dwa różne od siebie pojęcia, posiadające zupełnie odmienne znaczenie, zostały przetłumaczone identycznie, tj. jako «autoryzacja». W konsekwencji, oparcie się na polskiej wersji PSD1 prowadziło do absurdalnych wniosków. Błąd w polskiej wersji językowej PSD1 przełożył się na jej wadliwą implementację w ramach UsłPłU".

3 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L 337 z 23.12.2015, s. 35) (dalej: dyrektywa PSD2).

4 Ustawa z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. poz. 1075).

z przyjęciem pakietu PSD3[5], czyli projektów dyrektywy PSD3[6] oraz rozporządzenia Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego i zmieniającego rozporządzenie (UE) nr 1093/2010 (rozporządzenie PSR)[7]. Podjęcie próby zwrócenia uwagi na zakresy obu pojęć – uwierzytelniania i autoryzacji – w nawiązaniu do kwestii nieautoryzowanych transakcji nie rozwieje zapewne wielu wątpliwości, ale może pozwoli na ponowne zweryfikowanie ich znaczenia przy kolejnej modyfikacji przepisów ustawy o usługach płatniczych po wejściu w życie pakietu PSD3. Poniższe rozważania będą stanowiły jedynie próbę zwrócenia uwagi na istotę problemu, z uwzględnieniem dotychczasowego podejścia oraz przyszłych zmian (po wejściu w życie pakietu PSD3).

Należy zacząć od doprecyzowania pojęcia „autoryzacji" jako terminu, który stanowi – jak się wydaje – przeciwieństwo pojęcia „nieautoryzowane". Mając na uwadze już prawie kilkunastoletnie funkcjonowanie przepisów ustawy z 2011 r. (z istotną zmianą w 2018 r.), bogate orzecznictwo w tym zakresie oraz praktykę rynku usług finansowych, można ponownie zweryfikować pojęcie nieautoryzowanych transakcji przy założeniu, że nie można przyjmować w sposób tak jednoznaczny, iż nieautoryzowane transakcje to jedynie takie transakcje, wobec których występuje brak autoryzacji.

5 Tzw. pakiet PSD3 obejmuje projekty dyrektywy PSD3, rozporządzenia PSR oraz rozporządzenia FIDA.

6 Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie usług płatniczych i usług związanych z pieniądzem elektronicznym w ramach rynku wewnętrznego, zmieniającej dyrektywę 98/26/WE i uchylającej dyrektywy (UE) 2015/2366 i 2009/110/WE, Bruksela, 28 czerwca 2023 r., COM(2023) 366 final, 2023/0209 (COD) (dalej: dyrektywa PSD3).

7 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego i zmieniającego rozporządzenie (UE) nr 1093/2010, Bruksela, 28 czerwca 2023 r., COM(2023) 367 final, 2023/0210 (COD) (dalej: rozporządzenie PSR); wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) nr 1095/2010 i (UE) 2022/2554, Bruksela, 28 czerwca 2023 r., COM(2023) 360 final, 2023/0205 (COD) (rozporządzenie FIDA).

2 | Autoryzacja

Jak wskazuje art. 40 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2026 r., poz. 623; dalej: u.u.p.) i jak przyjęto w orzecznictwie, „stosownie do art. 40 ust. 1 ustawy 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 stanowi oświadczenie woli w rozumieniu art. 60 k.c. Z powyższego wynika więc, że transakcja płatnicza będzie uznana za nieautoryzowaną, jeżeli użytkownik nie wyraził zgody na jej wykonanie w sposób przewidziany w umowie, a więc również wtedy, gdy w ogóle nie wyraził zgody na wykonanie takiej transakcji płatniczej, gdyż została wyrażona przez osobę nieuprawnioną”[8].

Mając na uwadze powyższe, w oparciu o art. 40 u.u.p. autoryzacja to wyrażenie zgody przez osobę uprawnioną na dokonanie transakcji w sposób, jaki został ustalony w umowie. Tak jasno sformułowane stwierdzenie nie powinno budzić wątpliwości. Jak podnosi się w literaturze, „autoryzacja jest równoznaczna ze zgodą płatnika i że to zgoda, a nie żaden inny element, stanowi jedyną przesłankę uznania transakcji za autoryzowaną. Taka jest również jednolita konkluzja wynikająca z wykładni językowej art. 64 ust. 1 PSD2, którego implementację stanowi art. 40 ust. 1 u.u.p.”[9].

Zwraca jednak uwagę to, że o ile autoryzacja to wyrażenie zgody, o tyle w odniesieniu do pojęcia transakcji nieautoryzowanych należy rozważyć wiele sytuacji i okoliczności. Jeśli płatnik kwestionuje fakt wyrażenia zgody, to należy ocenić, czy i w jakich okolicznościach nastąpiło złożenie oświadczenia, które odpowiada ustalonym wymogom wyrażania zgody przez płatnika. Jeśli bowiem doszło do zrealizowania transakcji przez płatnika, to taka „zgoda” musiała być wyrażona. Ocena okoliczności wyrażenia takiej zgody – czy przez osobę uprawnioną, ale w okolicznościach dotkniętych wadliwością, czy też przez osobę nieuprawnioną, ale w oparciu o prawidłowo (zgodnie ze sposobem ustalonym w umowie) wyrażoną zgodę – ma zasadnicze znaczenie dla zakwalifikowania transakcji jako nieautoryzowanych.

8 Wyrok Sądu Okręgowego w Gliwicach z dnia 23 maja 2017 r., II C 421/16, LEX nr 2331891.

9 Maciej Juzoń, „Autoryzacja transakcji płatniczych w świetle przepisów i stanowiska UOKiK” *Monitor Prawa Bankowego*, nr 5 (2026): 23–37 i wskazana tam literatura.

Tak jasno więc sformułowane stwierdzenie, że transakcja jest uznawana za autoryzowaną, gdy płatnik wyraził na nią zgodę w sposób ustalony w umowie, w praktyce budzi również pewne wątpliwości w aspekcie nieautoryzowanych transakcji.

3 Uwierzytelnianie

Pojęcie uwierzytelniania zostało określone w ustawie o usługach płatniczych. Zgodnie z art. 2 pkt 33b u.u.p. uwierzytelnianie stanowi „procedurę umożliwiającą dostawcy usług płatniczych weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających". Uwierzytelnianie oznacza zatem – według literalnego brzmienia tej normy – „weryfikację tożsamości" lub weryfikację „ważności stosowania konkretnego instrumentu płatniczego". Aby uwierzytelnienie było możliwe, konieczne jest skorzystanie z indywidualnych danych uwierzytelniających.

Z kolei w ujęciu art. 2 pkt 9d u.u.p. przez indywidualne dane uwierzytelniające należy rozumieć „indywidualne dane zapewniane użytkownikowi przez dostawcę usług płatniczych do celów uwierzytelnienia". W oparciu o powyższe definicje ustawowe można wnioskować, że uwierzytelnianie to weryfikacja tożsamości, jak też ważności instrumentu płatniczego – brzmienie przepisu nie wyklucza bowiem, że może dojść do weryfikacji zarówno tożsamości, jak i ważności stosowanego instrumentu – oraz że proces ten przebiega według ustalonej procedury po to, aby dostawca mógł zweryfikować tożsamość użytkownika lub ważność stosowanego instrumentu płatniczego.

W ustawie o usługach płatniczych mowa jest również o silnym uwierzytelnianiu, o czym należy wspomnieć. Elementy pozwalające na silne uwierzytelnianie użytkownika (SCA) cechują się tym, że wykorzystywane są dwa elementy ściśle związane z osobą użytkownika, pozwalające na jego zweryfikowanie czy potwierdzenie jego tożsamości, czyli uwierzytelnienie – pod warunkiem, że nie doszło do ich udostępnienia, świadomego czy wymuszonego (np. wiedza o czymś, o czym wie wyłącznie użytkownik).

Zgodnie z art. 2 pkt 26aa u.u.p. przez silne uwierzytelnianie użytkownika należy rozumieć „uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:

a) wiedza o czymś, o czym wie wyłącznie użytkownik,

b) posiadanie czegoś, co posiada wyłącznie użytkownik,

c) cechy charakterystyczne użytkownika

– będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych".

Silne uwierzytelnianie ma służyć określonym celom – wzmocnieniu bezpieczeństwa realizacji transakcji płatniczej poprzez wymóg zastosowania co najmniej dwóch elementów przy uwierzytelnianiu użytkownika. Nie zmienia to jednak istoty uwierzytelniania ani silnego uwierzytelniania.

Mając na uwadze zacytowane powyżej przepisy ustawy o usługach płatniczych, z tak – jak się wydaje – jednoznacznego sformułowania należy rozumieć, że uwierzytelnianie służy przede wszystkim weryfikacji tożsamości, a w przypadku instrumentu płatniczego – weryfikacji jego ważności. Tak też sformułowanie to było interpretowane w orzecznictwie[10] oraz w literaturze[11]. Stwierdza się także, że „Uwierzytelnianie jest elementem procesu weryfikacji przez dostawcę usług płatniczych faktu wyrażenia przez płatnika zgody (autoryzacji) na wykonanie transakcji płatniczej, i jako takie, jest kluczową przesłanką dla udowodnienia przez dostawcę usług płatniczych, że transakcja została autoryzowana"[12].

Niewątpliwie proces uwierzytelniania służy do zweryfikowania tożsamości płatnika czy ważności wykorzystanego instrumentu, a powinno to nastąpić w aspekcie prawidłowo wyrażonej zgody – czyli weryfikacji, czy autoryzacja (wyrażenie zgody) nastąpiła przez podmiot uprawniony bądź z wykorzystaniem instrumentu płatniczego, który został wydany w tym celu i wykorzystany przez podmiot uprawniony. Jeśli bowiem proces weryfikacji tożsamości, czyli uwierzytelniania, potwierdzi, że przebiegł prawidłowo – zgodnie z ustalonymi przez strony zasadami – można przyjąć, że doszło również do prawidłowej autoryzacji transakcji, o ile do wyrażenia zgody na transakcję zastosowany został sposób ustalony przez strony w umowie. Od tej, wydawałoby się, prostej

10 Marta Fabiszewska, „Przegląd wybranego orzecznictwa w sprawach nieautoryzowanych transakcji płatniczych w latach 2021–2024" *internetowy Kwartalnik Antymonopolowy i Regulacyjny* 14, nr 1 (2025): 151–168; zob. również Bartosz Wyżykowski, „Przegląd aktualnego orzecznictwa w sprawach dotyczących nieautoryzowanych transakcji płatniczych" *Monitor Prawa Bankowego*, nr 9 (2020): 75–90.

11 Na temat autoryzacji i uwierzytelniania w aspekcie nieautoryzowanych transakcji zob. Grzegorz Ostaszewski, „Odpowiedzialność banku z tytułu nieautoryzowanych transakcji płatniczych" *Monitor Prawa Bankowego*, nr 3 (2024): 80–88.

12 Blocher, Iwański, „Nieautoryzowane transakcje płatnicze", 467.

zasady należy przewidzieć również szczególne sytuacje, gdy proces uwierzytelniania i autoryzacji dotknięty jest wadliwością. Pod pojęciem „wadliwości" należałoby przy tym rozumieć takie okoliczności, które wpływają na zaburzenie prawidłowości autoryzacji i uwierzytelniania. Mogą one być niezależne od płatnika (bowiem doszło np. do utraty instrumentu wraz z danymi), jak też całkowicie od niego zależne czy wręcz zamierzone (np. przekazanie instrumentu płatniczego wraz ze stosownymi indywidualnymi danymi uwierzytelniającymi osobie trzeciej).

Zgodzić się należy, że proces uwierzytelniania należy ujmować nie tylko jako weryfikację tożsamości *sensu stricto*, tak jak sugerowałoby literalne brzmienie przepisu, ale w szerszym aspekcie procesu realizacji elektronicznej transakcji płatniczej – przy założeniu, że prawidłowo wykonana elektroniczna transakcja płatnicza wymaga autoryzacji i uwierzytelnienia, a więc są to powiązane i wzajemnie uzależnione etapy procesu realizacji transakcji płatniczej. Prawidłowy przebieg procesu transakcji wymaga wyrażenia zgody na nią, czyli autoryzacji, przez podmiot, który został zweryfikowany jako uprawniony do jej dokonania, czyli został uwierzytelniony.

Jak wobec tego należałoby rozumieć transakcje nieautoryzowane? Czy tylko jako takie transakcje, na które płatnik nie wyraził zgody, czy też mogą to być również takie, w przypadku których doszło wprawdzie do prawidłowego uwierzytelnienia, ale nie zostały autoryzowane przez płatnika, jak i te, wobec których nastąpiła autoryzacja w sposób określony w umowie, a mimo to są one kwestionowane przez płatnika? Problem nieautoryzowanych transakcji skupia się przede wszystkim na ustaleniu zakresu i okoliczności wystąpienia braku zgody płatnika, gdy na taki brak zgody wskazuje płatnik, choć z formalnego punktu widzenia zgoda została wyrażona.

4 Autoryzacja a uwierzytelnianie wobec nieautoryzowanych transakcji

Mając na uwadze proces uwierzytelniania i autoryzacji, należy zwrócić uwagę na kilka aspektów prawnych, które zostały zresztą dostrzeżone również w orzecznictwie i doktrynie. Jak podkreśla SN, „wykazanie uwierzytelnienia przez dostawcę usług nie jest równoznaczne z wykazaniem autoryzacji, co potwierdza art. 45 ust. 2 u.u.p., który stanowi, iż wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do

udowodnienia, że transakcja płatnicza została przez użytkownika [autoryzowana]". Cytując dalej: „Wprawdzie część doktryny zwraca uwagę, że wykazanie przez dostawcę uwierzytelnienia przenosi ciężar dowodu co do braku autoryzacji na użytkownika (płatnika), jednakże *in casu* jest to pozbawione znaczenia, ponieważ Sąd odwoławczy ustalił jednoznacznie, iż powód nie udzielił zgody na przedmiotowe przelewy, a więc ich nie autoryzował. Rzecz bowiem w tym, że kod z obu SMS przesłanych przez Bank został użyty przez powoda z intencją zalogowania (był przezeń wpisywany na fałszywej stronie internetowej w celu zalogowania), a nie w celu autoryzacji przyszłych przelewów przez dodanie odbiorcy zaufanego"[13].

Jeśli jednak przyjąć, że po stwierdzeniu prawidłowego uwierzytelnienia to na płatniku spoczywa ciężar udowodnienia, że nie doszło do autoryzacji transakcji, nasuwa się pytanie, czy nie dochodzi do zmiany intencji rozwiązań prawnych przyjętych w dyrektywach PSD1 i PSD2. Ideą przyjętych rozwiązań było zwolnienie płatnika, który zgłasza wystąpienie nieautoryzowanych transakcji, z ciężaru dowodu i przeniesienie na podmiot świadczący usługi płatnicze – czyli profesjonalistę odpowiedzialnego również za zapewnienie bezpieczeństwa transakcji – obowiązku wykazania, iż doszło do prawidłowej autoryzacji. Oczywiście od tej prokonsumenckiej zasady mogą występować odstępstwa – nie powinno się chronić tych użytkowników, którzy kwestionują transakcje, do których doszło w wyniku ich rażącego niedbalstwa, świadomie czy z zamiarem oszukańczym, choć to właśnie im powinno to zostać udowodnione. Wobec tego czy faktycznie zasada odwróconego ciężaru dowodu służy tym użytkownikom, którzy zostali pokrzywdzeni?

Mając na uwadze zacytowane powyżej stanowisko SN, należy podkreślić, że nie powinno się utożsamiać autoryzacji z faktem zarejestrowanego użycia instrumentu płatniczego – co znalazło już potwierdzenie zarówno w literaturze, jak i w orzecznictwie, a przede wszystkim wynika z treści przepisów. Rozwiązanie to nie jest jednak także pozbawione wątpliwości. Stąd w projekcie pakietu PSD3 podjęto próbę doprecyzowania.

W projekcie rozporządzenia PSR przyjmuje się: „Transakcja płatnicza lub kilka transakcji płatniczych mogą być autoryzowane wyłącznie wówczas, gdy płatnik udzielił zezwolenia na wykonanie transakcji płatniczej". Umowa może

13 Wyrok SN z dnia 15 września 2023 r., II CSKP 1013/22, OSNC 2024, nr 6, poz. 61.

przy tym przewidywać, że autoryzacja może nastąpić po zrealizowaniu transakcji[14].

Zwraca uwagę to, że transakcja może być uznana za autoryzowaną, jeśli płatnik udzielił zezwolenia na jej wykonanie – z tak sformułowanej normy wynika przede wszystkim, że konieczne jest udzielenie zezwolenia na wykonanie transakcji. Zastanawia, czy możliwe jest, że nie dojdzie do uznania transakcji za autoryzowaną, mimo że płatnik udzielił zezwolenia na jej dokonanie. Czy występuje automatyczne zrównanie autoryzacji z zezwoleniem (tak jak ujmuje to aktualnie obowiązujący art. 40 u.u.p., zgodnie z którym – jak się przyjmuje – autoryzacja oznacza, że płatnik wyraził zgodę, a w projekcie rozporządzenia stwierdza się, że transakcja może być uznana za autoryzowaną wyłącznie wówczas, gdy płatnik udzielił na nią zezwolenia)? Z całą pewnością należy uznać, że ocena, czy transakcja będzie autoryzowana, jest uzależniona od tego, czy płatnik udzielił zezwolenia – przed zrealizowaniem transakcji albo po nim. Przy czym zezwolenia udzielić powinien podmiot zweryfikowany, czyli już po uwierzytelnieniu (*authentication*) – po zweryfikowaniu tożsamości użytkownika usług płatniczych, a więc po zweryfikowaniu, że zezwolenia udziela osoba uprawniona. Stąd trudno oddzielić proces uwierzytelniania od procesu wyrażenia zezwolenia. Gdy oba procesy przebiegną prawidłowo, wydaje się, że można stwierdzić, iż transakcja jest autoryzowana. Mimo że ani dotychczasowe regulacje, ani projekt pakietu PSD3 nie wskazują tego jednoznacznie, wydaje się, że przyjęcie, iż transakcja jest autoryzowana, bowiem płatnik udzielił zezwolenia, następuje wraz ze zweryfikowaniem tożsamości płatnika (w ujęciu projektu rozporządzenia PSR „uwierzytelnianie" oznacza „procedurę umożliwiającą dostawcy usług płatniczych weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika")[15]. Zezwolenia na dokonanie transakcji (przed jej dokonaniem czy też po nim) może zaś udzielić tylko podmiot do tego uprawniony, czyli zweryfikowany poprzez uwierzytelnienie.

Pozostaje kwestia tych transakcji płatniczych, kwestionowanych przez płatnika, co do których nastąpiła autoryzacja (i, jak przyjmuje projekt rozporządzenia PSR, „transakcja ta została autoryzowana, dokładnie zapisana, ujęta w księgach i że na transakcję nie miała wpływu awaria techniczna ani

14 Art. 49 ust. 1 projektu rozporządzenia PSR.
15 Art. 3 pkt 34 projektu rozporządzenia PSR.

innego rodzaju usterka związana z usługą świadczoną przez danego dostawcę usług płatniczych"). Oznacza to, że doszło do wyrażenia zgody na transakcję (zezwolenia według projektu), następnie transakcja została zapisana i ujęta w księgach, a więc proces zainicjowania transakcji oraz jej realizacji przebiegł prawidłowo – czyli zgodnie ze sposobem ustalonym w umowie zawartej pomiędzy dostawcą a płatnikiem. Ponadto na wadliwość transakcji nie mogła mieć wpływu awaria techniczna czy też innego rodzaju usterka związana z realizacją transakcji. A jednak płatnik ją kwestionuje i zgłasza jako nieautoryzowaną. Ze sformułowania projektu rozporządzenia wynika, że w sytuacjach, gdy płatnik kwestionuje takie transakcje (na które udzielono zezwolenia i które zostały zapisane oraz ujęte w księgach), to dostawca winien udowodnić, że doszło do prawidłowej autoryzacji, czyli że to płatnik udzielił zezwolenia na transakcję, co następnie spowodowało, że transakcja została zapisana i ujęta w księgach, oraz że nie było żadnej awarii ani uchybienia w działaniu systemu, które mogłyby wpłynąć na proces realizacji transakcji. Pozostaje tylko zastanowić się, czy w takich okolicznościach zwrot kończący zacytowany przepis projektu rozporządzenia – „innego rodzaju usterka związana z usługą świadczoną" – pozostanie „furtką", która obejmie różnego rodzaju działania natury przestępczej (np. podesłanie łudząco podobnej strony internetowej banku, co w przypadku transakcji, na które udzielono zgody/zezwolenia, może mieć miejsce).

W projekcie rozporządzenia PSR uregulowano przy tym wyraźnie jeden z przypadków, gdy dojdzie do – jak przyjmuje projekt w art. 59 ust. 1 – zmanipulowania płatnika: „1. Jeżeli użytkownik usług płatniczych będący konsumentem uległ manipulacji osoby trzeciej udającej pracownika dostawcy usług płatniczych konsumenta, bezprawnie wykorzystującej nazwisko lub nazwę bądź adres e-mail lub numer telefonu tego dostawcy usług płatniczych, a w wyniku tej manipulacji doszło następnie do nielegalnych autoryzowanych transakcji płatniczych, dostawca usług płatniczych zwróci konsumentowi pełną kwotę nielegalnej autoryzowanej transakcji płatniczej pod warunkiem, że konsument niezwłocznie zgłosił oszustwo policji oraz powiadomił dostawcę usług płatniczych"[16].

16 Art. 59 ust. 2 projektu rozporządzenia PSR: „W terminie 10 dni roboczych po odnotowaniu nielegalnej autoryzowanej transakcji płatniczej lub po otrzymaniu stosownego zgłoszenia dostawca usług płatniczych podejmuje jedno z następujących działań: a) dokonuje na rzecz konsumenta zwrotu kwoty nielegalnej autoryzowanej

Jeśli przyjmiemy, że dostawca po zgłoszeniu przez płatnika wystąpienia nieautoryzowanych transakcji ma obowiązek niezwłocznie zwrócić kwoty kwestionowanych transakcji[17] – niezależnie od późniejszych ustaleń co do okoliczności wystąpienia „wadliwości" transakcji (z wyjątkiem okoliczności ewidentnie wskazujących na zamiar oszukańczy, na co dostawca musiałby mieć dowody) – to przerzucenie na dostawcę ciężaru dowodu wykazania wyrażenia przez płatnika zezwolenia (obecnie: zgody) na wykonanie transakcji ma sens. Dostawca zobowiązany do niezwłocznego[18] – po zgłoszeniu – zwrotu kwot kwestionowanych transakcji płatniczych (jako nieautoryzowanych), po zrealizowaniu tego obowiązku będzie w szczególności zainteresowany ustaleniem okoliczności i przyczyn zgłoszenia przez płatnika tych transakcji jako przez niego nieautoryzowanych. Należy przy tym zwrócić uwagę, że obowiązek zwrotu kwot transakcji kwestionowanych jako nieautoryzowane, z pewnymi wyjątkami (które powinny zostać przez dostawcę udowodnione), wynika też z treści aktualnie obowiązujących przepisów ustawy o usługach płatniczych[19] (i jest potwierdzony w pakiecie PSD3). Wówczas dostawca będzie zainteresowany wykazaniem okoliczności zwalniających go od odpowiedzialności poprzez

---

transakcji płatniczej; b) jeżeli dostawca usług płatniczych ma uzasadnione podstawy, aby podejrzewać, że konsument popełnił oszustwo lub dopuścił się rażącego niedbalstwa, przekazuje konsumentowi uzasadnienie odmowy dokonania zwrotu i wskazuje organy, do których konsument może skierować sprawę zgodnie z art. 90, 91, 93, 94 i 95, jeżeli konsument nie zgadza się z przedstawionym uzasadnieniem. 3. Ustępu 1 nie stosuje się, jeżeli konsument działał w nieuczciwych zamiarach lub dopuścił się rażącego niedbalstwa".

17 Tak przyjmuje projekt rozporządzenia PSR w art. 56 ust. 1; dla porównania tak aktualnie art. 46 ust. 1 u.u.p.

18 Według zasady D+1.

19 Art. 46 ust. 1 u.u.p.: „Z zastrzeżeniem art. 44 ust. 2, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika niezwłocznie, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwraca płatnikowi kwotę nieautoryzowanej transakcji płatniczej, z wyjątkiem przypadku gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw. W przypadku gdy płatnik korzysta z rachunku płatniczego, dostawca płatnika przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. Data waluty w odniesieniu do uznania rachunku płatniczego płatnika nie może być późniejsza od daty obciążenia tą kwotą".

wykazanie, że doszło do autoryzacji. Wówczas też idea przerzucenia ciężaru dowodu z podmiotu poszkodowanego na dostawcę ma sens w aspekcie ochrony praw konsumenta[20].

5 Podsumowanie

Mając na uwadze powyższe uwagi, trudno jednoznacznie wskazać schemat, który „ułatwiłby" ustalenie znaczenia i zakresu pojęcia „nieautoryzowane transakcje", tym bardziej że nie można przyjmować w sposób automatyczny, iż są to jedynie transakcje, na które płatnik nie wyraził zgody. Niewątpliwie w przygotowanym pakiecie PSD3, w szczególności w projekcie rozporządzenia PSR, podjęte zostały próby doprecyzowania okoliczności, które mogą wskazywać, że mimo wyrażenia zezwolenia przez płatnika, czyli autoryzacji, można uznać transakcję za nieautoryzowaną – wówczas gdy wystąpią okoliczności tzw. manipulowania przez osoby trzecie – co należy uznać za rozwiązanie pozytywne, mając na uwadze coraz częstsze takie przypadki. W tym wypadku płatnik, choć z formalnego punktu widzenia wyraził zgodę, został wprowadzony w błąd, a jego oświadczenie dotknięte jest nieważnością względną. Z kolei zarzut niezachowania należytej staranności przez płatnika w sytuacjach zmanipulowania przez osoby trzecie nie zawsze może być uzasadniony, biorąc pod uwagę „dobre", wręcz profesjonalne przygotowanie osób, które manipulują płatnikiem, oraz niekiedy brak wiedzy płatnika na takim poziomie technologicznym, który pozwalałby na dostrzeżenie, iż ma on do czynienia nie z dostawcą, lecz z osobą trzecią.

Niewątpliwie kwestia nieautoryzowanych transakcji wymaga indywidualnej oceny w każdym przypadku. Sformułowanie „nieautoryzowane transakcje" obejmuje cały katalog przypadków, z których część stanowią także te transakcje, które spełniają wymogi autoryzacji i uwierzytelnienia i na które została wprawdzie wyrażona zgoda, ale w okolicznościach wskazujących na wadliwość.

20 Kwestia ta stała się przedmiotem oceny Prezesa UOKiK, zob. Stanowisko Prezesa UOKiK w sprawie interpretacji przepisów ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych w zakresie dotyczącym nieautoryzowanych transakcji płatniczych, opublikowane jako „Nieautoryzowane transakcje płatnicze. Stanowisko Prezesa UOKiK" *Monitor Prawa Bankowego*, nr 2 (2023): 5–13.

Dopiero ocena okoliczności wyrażenia zgody (zezwolenia – w ujęciu projektu rozporządzenia PSR) przez płatnika pozwoli na zakwalifikowanie danej transakcji do katalogu transakcji nieautoryzowanych, z pełną tego konsekwencją w zakresie odpowiedzialności dostawcy.

Bibliografia

Blocher, Marcin, Wojciech Iwański. „Nieautoryzowane transakcje płatnicze" *Monitor Prawniczy*, nr 9 (2020): 465–471.

Fabiszewska, Marta. „Przegląd wybranego orzecznictwa w sprawach nieautoryzowanych transakcji płatniczych w latach 2021–2024" *internetowy Kwartalnik Antymonopolowy i Regulacyjny* 14, nr 1 (2025): 151–168.

Juzoń, Maciej. „Autoryzacja transakcji płatniczych w świetle przepisów i stanowiska UOKiK" *Monitor Prawa Bankowego*, nr 5 (2026): 23–37.

„Nieautoryzowane transakcje płatnicze. Stanowisko Prezesa UOKiK" *Monitor Prawa Bankowego*, nr 2 (2023): 5–13.

Ostaszewski, Grzegorz. „Odpowiedzialność banku z tytułu nieautoryzowanych transakcji płatniczych" *Monitor Prawa Bankowego*, nr 3 (2024): 80–88.

Wyżykowski, Bartosz. „Przegląd aktualnego orzecznictwa w sprawach dotyczących nieautoryzowanych transakcji płatniczych" *Monitor Prawa Bankowego*, nr 9 (2020): 75–90.