Bartosz Wyżykowski*

Spory między dostawcami usług płatniczych a użytkownikami dotyczące transakcji płatniczych w świetle najnowszego orzecznictwa polskich sądów powszechnych

Spis treści

I. Wprowadzenie
II. Nieautoryzowana transakcja płatnicza a transakcja płatnicza wykonana z podaniem nieprawidłowego unikatowego identyfikatora
III. Przegląd wybranych orzeczeń wydanych w sprawach dotyczących transakcji płatniczych
1. Wyrok Sądu Apelacyjnego w Warszawie z 8 października 2021 r., VII Aga 228/20
2. Wyrok Sądu Okręgowego w Olsztynie z 28 stycznia 2022 r., V Ga 328/21
3. Wyrok Sądu Okręgowego w Poznaniu z 24 września 2021 r., XV Ca 378/21
4. Wyrok Sądu Okręgowego w Łodzi z 27 lipca 2021 r., XIII Ga 833/20
5. Wyrok Sądu Rejonowego Poznań-Stare Miasto w Poznaniu z 8 grudnia 2021 r., I C 648/20
6. Wyrok Sądu Rejonowego Szczecin-Centrum w Szczecinie z 7 czerwca 2021 r., XI GC 617/20
7. Wyrok Sądu Rejonowego dla Łodzi-Widzewa z 17 lutego 2021 r., VIII C 873/18
IV. Podsumowanie

Streszczenie

Naturalną konsekwencją coraz powszechniejszego wykorzystywania nowoczesnych form płatności jest rozwój przestępczości w tym obszarze. W rezultacie coraz bardziej doniosłą – zarówno prawnie, jak i społecznie – jest problematyka rozkładu ryzyka i odpowiedzialności z tytułu nieautoryzowanych transakcji płatniczych. W artykule dokonano przeglądu wybranych prawomocnych orzeczeń polskich sądów powszechnych w sprawach, których przedmiotem sporu były transakcje płatnicze.

Słowa kluczowe: nieautoryzowana transakcja płatnicza; nieprawidłowy unikatowy identyfikator; użytkownik; dostawca usług płatniczych, bank, konsument.

JEL: K12, K15, K23, K24, K41, K42

* Doktor nauk prawnych; radca prawny w DLK Legal Korus sp.k.; artykuł prezentuje poglądy autora i nie powinien być traktowany jako stanowisko innych podmiotów, organów lub instytucji.

I. Wprowadzenie

Innowacyjny charakter rynku usług płatniczych skutkuje nieustannym wzrostem liczby transakcji płatniczych, w tym z wykorzystaniem nowych technologii. Świadczy o tym pojawienie się w ostatnich latach nowych metod płatności, takich jak BLIK[1], metoda *pay-by-link*[2] czy nowy rodzaj usługi płatniczej, jaką jest usługa inicjowania transakcji płatniczej[3] (*payment initiation service*). W szczególności dostrzegalny jest szybki rozwój płatności elektronicznych i zdalnych, w tym zwłaszcza mobilnych, a więc z wykorzystaniem telefonów komórkowych (smartfonów). W rezultacie na rynku usług finansowych wyodrębniła się nowa kategoria klientów (*mobile only*), którzy nie korzystają już z innych, poza mobilnym, kanałów dostępu (Rutkowska-Tomaszewska, 2021, s. 5).

Innowacje technologiczne są siłą napędową rozwoju sektora finansowego, oznaczają jednak również występowanie wielu rodzajów ryzyka, zagrożeń związanych z cyberprzestrzenią, ochroną danych konsumentów i inwestorów oraz integralności rynku finansowego (Rutkowska-Tomaszewska, 2021a, s. 9). Konsekwencją coraz powszechniejszego wykorzystywania nowoczesnych form płatności jest rozwój przestępczości w tym obszarze (Grabowski, 2016). Większe jest bowiem ryzyko wystąpienia nadużyć i transakcji nieautoryzowanych spowodowanych weryfikacją tożsamości klienta przez zautomatyzowane mechanizmy (Bodzioch, 2014).

Z informacji publikowanych przez CERT Polska[4] wynika, że w 2021 r. CERT Polska zarejestrował łącznie 29 483 unikalnych incydentów cyberbezpieczeństwa[5]. Odnotowano wzrost obsłużonych incydentów o 182% w porównaniu z rokiem 2020[6]. Najczęstszym typem był *phishing*[7] – stanowiący aż 76,57% wszystkich obsłużonych incydentów[8]. Jest to wzrost o 196% w porównaniu z poprzednim rokiem[9]. Sektory gospodarki, których najczęściej dotyczyły incydenty to: media, handel hurtowy i detaliczny oraz poczta i usługi kurierskie[10]. Przestępcy skupili się na udoskonalaniu znanych scenariuszy *phishingowych*: przejęciu kont na Facebooku, fałszywych bramkach płatności oraz wyłudzaniu pieniędzy od sprzedających na portalach ogłoszeniowych[11]. Z kolei z danych podawanych przez NBP wynika, że w drugim półroczu 2021 r. według informacji przekazywanych przez banki, liczba operacji oszukańczych dokonanych kartami płatniczymi wyniosła 121 700, natomiast według informacji otrzymanych od agentów rozliczeniowych liczba

[1] Przez BLIK należy rozumieć zarówno aplikację, niekartowy schemat płatniczy, jak i system płatności stworzony przez Polski Standard Płatności sp. z o.o. Umożliwia on użytkownikom smartfonów inicjowanie różnego typu transakcji za pomocą aplikacji generującej jednorazowe sześciocyfrowe kody służące do autoryzacji tych operacji.

[2] Przez pojęcie *pay-by-link* rozumie się przelew bezpośredni uruchamiany specjalnie wygenerowanym linkiem. Wszystkie dane potrzebne do wykonania przelewu są wypełniane automatycznie, a klient musi tylko zatwierdzić przelew w systemie bankowości internetowej (Balkowski, 2018, s. 7).

[3] Ustawa z dnia 19.08.2011 r. o usługach płatniczych (Dz. U. 2011 Nr 199 poz. 1175; t.j.: Dz. U. 2022 poz. 2360, 2640), art. 3 ust. 1 pkt 7 w zw. z ust. 5 (dalej: uup) oraz Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25.11.2015 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 (OJ L 337, 23.12.2015, p. 35–127), art. 4 pkt 15 (dalej: PSD2).

[4] Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne, zob. https://www.cert.pl/o-nas/ (31.07.2022).

[5] Raport roczny 2021 z działalności CERT Polska, „Krajobraz bezpieczeństwa polskiego internetu", s. 12 i 20. Pozyskano z: https://cert.pl/uploads/docs/Raport_CP_2021.pdf (31.07.2022).

[6] Ibidem.

[7] Przez pojęcie *phihingu* rozumie się metodę oszustwa, w której dany podmiot (przestępca) podszywa się pod inny podmiot w celu wyłudzenia określonych informacji (np. indywidulnych danych uwierzytelniających) lub nakłonienia ofiary do realizacji określonych działań (Górnisiewicz, Obczyński i Pstruś, 2014, s. 7; podobnie: Müller-Brockhausen, 2014, s. 91, pkt 138). Istnieje również tzw. *spearphishing*, czyli forma *phishingu* nacelowana na daną osobę (Hadnagy i Fincher, 2017, s. 28).

[8] Raport roczny 2021 z działalności CERT Polska (…), op. cit., s. 12 i 20.

[9] Ibidem.

[10] Ibidem.

[11] Ibidem, s.12.

ta osiągnęła poziom 19 500[12]. W drugim półroczu 2021 r. średnia wartość transakcji oszukańczej dokonanej kartą płatniczą wynosiła 354,4 zł i była wyższa o 11,5% w stosunku do poprzedniego półrocza (w poprzednim półroczu wynosiła ona 317,7 zł)[13].

Celem niniejszego artykułu jest dokonanie przeglądu wybranych prawomocnych na dzień 30 czerwca 2022 r. orzeczeń sądów powszechnych wydanych w okresie między 1 stycznia 2021 r. a 30 czerwca 2022 r. w sprawach, których przedmiotem sporu były transakcje płatnicze[14]. Najczęściej chodzi o spory między bankami a użytkownikami rozstrzygane na podstawie przepisów uup, która stanowi implementację PSD2. Wobec tego, że na gruncie przepisów uup bank stanowi kategorię dostawcy usług płatniczych, w dalszej części artykułu mowa będzie również ogólnie o dostawcach. Z kolei dla określenia użytkowników (płatników), w tym konsumentów mowa będzie o klientach. Orzeczenia omówiono począwszy od najwyższej do najniższej instancji, następnie uwzględniając daty ich wydania, począwszy od orzeczenia najbardziej aktualnego. Przegląd nie obejmuje orzeczeń SN ani TSUE, gdyż brakuje wypowiedzi tych sądów odnoszących się ściśle do problematyki rozkładu odpowiedzialności za wykonanie transakcji płatniczych w badanym okresie.

II. Nieautoryzowana transakcja płatnicza a transakcja płatnicza wykonana z podaniem nieprawidłowego unikatowego identyfikatora

Przed przejściem do właściwego przeglądu orzecznictwa, koniecznym jest krótkie wyjaśnienie różnicy między nieautoryzowaną transakcją płatniczą a transakcją wykonaną z podaniem nieprawidłowego unikatowego identyfikatora. Większość sporów dotyczy właśnie tych zagadnień. Pomimo że uup nie definiuje nieautoryzowanej transakcji płatniczej, *de lege lata* należy przyjąć, że chodzi o transakcję, na którą płatnik nie wyraził zgody w sposób wskazany w umowie[15] (tak też: Bajor, 2017, komentarz do art. 46). Potwierdza to wprost art. 64 ust. 2 zd. 3 PSD2, zgodnie z którym w przypadku braku zgody transakcję płatniczą uznaje się za nieautoryzowaną[16].

Okoliczność, że płatnik twierdzi, jakoby transakcja ma charakter nieautoryzowany, w żadnym razie nie musi zatem oznaczać, że tak faktycznie jest. Wyraźnie przesądza to również prawodawca unijny w motywie 70 zd. 1 PSD2. Nie ma on zatem żadnych wątpliwości, iż treść zgłoszenia (reklamacji) klienta w żadnym razie nie przesądza czy reklamowana przez klienta transakcja istotnie nie została autoryzowana. W zakresie, w jakim dostawca rozpatruje zgłoszenie lub reklamację płatnika, na podstawie dokonywanych przez siebie ustaleń, podejmuje on decyzję gospodarczą w przedmiocie rozstrzygnięcia reklamacji, a więc również w przedmiocie tego czy transakcję uznaje za autoryzowaną, czy też nieautoryzowaną (Wyżykowski, 2019, s. 114).

Z perspektywy dostawcy transakcja zostaje prawidłowo autoryzowana, gdy ten stwierdzi, że transakcja została uwierzytelniona (czy zastosowano silne uwierzytelnianie użytkownika (SCA), tam gdzie było to wymagane na podstawie obowiązujących przepisów), prawidłowo zapisana

[12] Narodowy Bank Polski, Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2021 r., kwiecień 2022. Departament Systemu Płatniczego. Warszawa 2021, s. 124. Pozyskano z: https://www.nbp.pl/systemplatniczy/ocena/ocena2021_2.pdf (31.07.2022). Z uwagi na różny zakres danych dotyczących oszustw dokonywanych kartami płatniczymi ujmowanych w sprawozdaniach, w sposób naturalny od lat występuje rozbieżność w danych przekazywanych przez agentów rozliczeniowych oraz banki (s. 117).

[13] Ibidem, s. 121.

[14] Dokonano przeglądu prawomocnych orzeczeń sądów powszechnych wydanych między 1 stycznia 2021 r. a 30 czerwca 2022 r. wyszukanych po słowach „nieautoryzowana" oraz „usługi płatnicze", udostępnionych na stronie pod linkiem: https://orzeczenia.ms.gov.pl/ (31.07.2022).

[15] Art. 40 ust. 1 zd. 1 uup – rozumowanie na zasadzie *a contrario*. Uproszczeniem jest zatem twierdzenie, że brak zgody skutkuje uznaniem transakcji za nieautoryzowaną (Wojtczak, 2012, s. 226). Chodzi o brak zgody wyrażony w sposób określony w umowie.

[16] Art. 64 ust. 2 zd. 3 PSD2.

w systemie służącym do obsługi transakcji płatniczych dostawcy, nie miała na nią wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą świadczoną przez tego dostawcę oraz gdy dostawca odnotował zaistnienie właściwej czynności konwencjonalnej określonej w umowie, a więc zgody na wykonanie transakcji. Z perspektywy dostawcy oznacza to, że zgodę na wykonanie transakcji wyraził płatnik[17]. Zarazem strony mogą uzgodnić w umowie, że czynność płatnika, która pozwala dostawcy na dokonanie uwierzytelnienia, stanowi jednocześnie zgodę na wykonanie transakcji, a więc jej autoryzację. W przypadku uznania przez dostawcę, że transakcja ma charakter nieautoryzowany, dodatkowo podejmuje on decyzję gospodarczą w przedmiocie tego czy ryzyko (odpowiedzialność) z tytułu transakcji nieautoryzowanej ponosi dostawca, czy też płatnik. Finalnie, gdy sprawa poddana zostanie rozpatrzeniu przez sąd, ustali on w sposób wiążący zaistniały stan faktyczny i kwalifikację prawną wykonanej transakcji.

W przypadku, gdy transakcja ma charakter autoryzowany, może się okazać, że płatnik w zleceniu płatniczym podał nieprawidłowy unikatowy identyfikator (najczęściej chodzi tu o numer rachunku bankowego/płatniczego). Wówczas zastosowanie znajdą art. 143–143c uup. W piśmiennictwie stwierdzono – moim zdaniem – błędnie, że przepisy te znajdą zastosowanie wyłączenie w przypadku braku zgodności unikatowego identyfikatora z pozostałymi danymi odbiorcy (Torończak, 2019, s. 77–78). Tymczasem, treść przepisów PSD2[18] oraz uup[19], jak również lektura uzasadnienia projektu nowelizacji uup, na mocy której dokonano implementacji art. 88 PSD2[20], nie dają podstaw to takiego wniosku. Przeciwnie, można wywodzić, że celem zarówno prawodawcy unijnego, jak i ustawodawcy polskiego było umożliwienie skorzystania z procedury mającej na celu odzyskanie środków mylnie zleconej transakcji, jak najszerszemu kręgowi płatników. Dlatego należy uznać, że z transakcją wykonaną z podaniem nieprawidłowego unikatowego identyfikatora będziemy mieli do czynienia wówczas, gdy w zleceniu płatniczym brak jest zgodności między danymi odbiorcy a unikatowym identyfikatorem, jak również wówczas, gdy podany przez płatnika identyfikator przypisany będzie do właściwego odbiorcy, lecz pomyłka płatnika dotyczyć będzie obu kategorii danych, tj. będzie on miał mylne wyobrażenie o odbiorcy (Wyżykowski, 2021, s. 47)[21].

III. Przegląd wybranych orzeczeń wydanych w sprawach dotyczących transakcji płatniczych

1. Wyrok Sądu Apelacyjnego w Warszawie z 8 października 2021 r., VII Aga 228/20

Komentowane orzeczenie wydane zostało w sprawie, w której przestępcy na wyłudzonym od usługodawcy (niedoszłego beneficjenta przelewu) duplikacie faktury dokonali podmiany banku i numeru rachunku, na który należało dokonać wpłaty i następnie przesłali tę fakturę drogą

[17] Podobnie w wyr. SO w Olsztynie z 22.01.2022 r., V Ga 328/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022), który będzie przedmiotem analizy w dalszej części artykułu, sąd ten stwierdził, że: „Zatem z punktu widzenia systemu bankowego sporna transakcja może być uznana za autoryzowaną bowiem została ona potwierdzona kodem przesłanym przez pozwanego w wiadomościach SMS". Ostatecznie jednak, sąd przyjął, iż: „Jednakże skoro autoryzacja tej transakcji została uzyskana poprzez doprowadzenie użytkownika bankowości elektronicznej (powoda) postępem do autoryzacji transakcji, której *de facto* nie chciał wykonać poprzez podmianę danych faktycznych odbiorcy to taka transakcja jest traktowana jako nieautoryzowana". Zagadnienie to jest przedmiotem szerszej analizy w dalszej części artykułu.

[18] Motyw 88 i art. 88 PSD2.

[19] Art. 143–143a uup.

[20] Przedstawiony przez Prezydenta Rzeczypospolitej Polskiej projekt ustawy o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw, druk sejmowy nr 1606, Sejm RP VIII kadencji. Zob. https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=1606 (31.07.2022).

[21] Co nie oznacza w sposób automatyczny, że mamy tu do czynienia z wadą oświadczenia woli.

elektroniczną do usługobiorcy, który miał dokonać zapłaty z tego tytułu[22]. Ten, mimo pewnych wątpliwości i próby nawiązania kontaktu z usługodawcą, celem potwierdzenia zmiany numeru rachunku, zainicjował przelew[23]. W dniu 24 sierpnia 2015 r. wykonany został przelew na kwotę 235 500 zł, przy czym w poleceniu (zleceniu) przelewu wskazany został podmieniony rachunek, natomiast jako beneficjent środków pieniężnych wskazany został niedoszły beneficjent przelewu, a więc podmiot inny niż ten, który był posiadaczem podstawionego rachunku[24]. Jak należy rozumieć z treści wyroku, usługodawca i usługobiorca wspólnie pozwali bank (dostawcę), w którym rachunek posiadał rzeczywisty beneficjent przelewu, a więc podmiot, którego rachunek uznany został kwotą spornej transakcji wykonanej wskutek manipulacji ze strony przestępców. Pozwanym nie był zatem bank, w którym usługobiorca jako klient zainicjował transakcję.

SA w Warszawie orzekł o odpowiedzialności pozwanego banku na podstawie art. 415 k.c., jednakże stwierdził, inaczej niż sąd I instancji, że źródła odpowiedzialności odszkodowawczej pozwanego należało upatrywać nie w otwarciu rachunku bankowego dla beneficjenta przelewu (ewentualnie osoby podającej się za beneficjenta)[25], ale w braku zachowania przez pozwany bank reguł ostrożności i szczególnej staranności przy wypłacie środków pieniężnych na rzecz beneficjenta[26]. W ocenie SA w Warszawie, bank, podejmując decyzję o wypłacie środków pieniężnych, naruszył ogólne zasady ustanawiające obowiązek banku do szczególnej dbałości o powierzone mu środki pieniężne i w rezultacie uznał, że bank ponosi odpowiedzialność za brak zachowania właściwej ostrożności przy podejmowaniu decyzji o wypłacie środków pieniężnych z rachunku bankowego, albowiem ustalone okoliczności sprawy wskazywały, że bank przed wypłatą środków pieniężnych powinien podjąć przynajmniej podstawowe czynności wyjaśniające[27]. SA w Warszawie zauważył, że na rachunek bankowy, z którego miały zostać wypłacone środki pieniężne na rzecz beneficjenta przelewu, wpłynęła znaczna kwota pieniężna, zaś w tytule jej przelewu został wskazany inny beneficjent niż składający dyspozycję wypłaty tych środków[28]. W tym stanie rzeczy złożenie przez posiadacza rachunku bankowego dyspozycji wypłaty jednorazowo znacznej części środków pieniężnych powinno skutkować podjęciem przez pracowników banku czynności weryfikujących tę operację[29]. Dodatkowo zauważyć należało, że na rachunek bankowy, z którego miały zostać wypłacone środki pieniężne, w całym dotychczasowym okresie jego istnienia, wpłynęła tylko jedna wpłata, nie były na nim przeprowadzane żadne transakcje, poza początkową wpłatą[30]. Nadto, rachunek został otworzony miesiąc wcześniej przez cudzoziemca, a wzór podpisu tej osoby obejmował jedynie imię[31]. Jednocześnie zdaniem sądu, w ślad za ustaleniami sądu

22 Wyr. SA w Warszawie z 8.10.2021 r., VII Aga 228/20. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

23 Ibidem.

24 Ibidem.

25 Z treści wyr. SA w Warszawie wynika, że rozpatrujący sprawę sąd I instancji uznał, że: „Przy uwzględnieniu treści art. 2 ust. 1 ustawy Prawo dewizowe oraz Regulaminu, Sąd Okręgowy uznał, że A. W. (1) posiadała na terenie Polski status nierezydenta z kraju trzeciego (posiadała obywatelstwo M.), co oznaczało, że w świetle zapisów Regulaminu nie posiadała uprawnienia do żądania otwarcia rachunku bankowego w pozwanym Banku. Oznaczało to, że Bank (...) nie dochował należytej staranności, otwierając rachunek bankowy osobie nieposiadającej statusu rezydenta na terenie Polski, w oparciu o niepodpisany paszport, dopuszczając się tym samym czynu zabronionego. Do takiego zachowania doszło na skutek przekroczenia obowiązujących u pozwanego wewnętrznych procedur w zakresie otwierania rachunków bankowych, co przesadzało o jego winie". Kwestie te nie są przedmiotem analizy w niniejszym artykule.

26 Wyr. SA w Warszawie z 8.10.2021 r., VII Aga 228/20. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

27 Ibidem.

28 Ibidem.

29 Ibidem.

30 Ibidem.

31 Ibidem.

I instancji, całokształt okoliczności sprawy uzasadniał przyjęcie, że przyczynienie się powodów do powstania szkody należało określić na poziomie 50%[32].

W tym kontekście warto poczynić kilka uwag. Należy odnotować, że sąd, powołując się na zasadę dbałości przez bank o powierzone mu środki pieniężne, w istocie powołuje się na zasadę, która w pierwszej kolejności ma na celu ochronę praw i interesów posiadacza rachunku. Tymczasem w komentowanym orzeczeniu przywoływana jest ona przez sąd dla uzasadnienia roszczeń innych uczestników obrotu bezgotówkowego, którzy nie są klientem pozwanego banku, albo ujmując to jeszcze ściślej, którzy nie kierują swoich roszczeń do banku z tytułu prowadzonego dla nich przez ten bank rachunku płatniczego. Dla uniknięcia wątpliwości, nie jest moją intencją, aby w tym aspekcie automatycznie krytykować podejście sądu. W doktrynie zwraca się uwagę, że na gruncie art. 50 ust. 2 pb[33] wcale nie jest oczywiste, co należy rozumieć przez nakaz dokładania szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych przez bank[34]. SA w Warszawie wywiódł zatem restrykcyjną normę postępowania, jaką jest zapewnienie szeroko rozumianego bezpieczeństwa przechowywanych środków pieniężnych[35], a więc z punktu widzenia praw i interesów szerszego kręgu posiadaczy rachunków (użytkowników usług płatniczych). Niemniej nie uzasadnił szerzej przyjętego wariantu interpretacyjnego.

Krytycznie należy natomiast ocenić zarzut sądu naruszenia przez bank reguł ostrożności i szczególnej staranności z uwagi na okoliczność, że w tytule przelewu został wskazany inny beneficjent niż składający dyspozycję wypłaty tych środków. W zakresie, w jakim zastosowanie znajdują przepisy uup (a wydaje się, że znajdywały one zastosowanie do spornej transakcji, choć jako podstawę roszczenia sąd przywołał przepisy ogólne k.c., co wynikało z okoliczności, że żaden z powodów nie był klientem pozwanego banku, a w rezultacie nie wiązała ich z tym dostawcą umowa o usługę płatniczą regulowana na mocy uup), *de lege lata* odpowiedzialność dostawców za wykonanie transakcji z podaniem nieprawidłowego unikatowego identyfikatora jest wyłączona[36] i *lege non distinguente* dotyczy to każdego dostawcy uczestniczącego w cyklu wykonania transakcji (cyklu rozliczeniowym), a więc również dostawcy, który prowadzi rachunek dla odbiorcy transakcji (Wyżykowski, 2021, s. 60)[37]. Z treści orzeczenia wynika, że okoliczność tę dostrzegł sąd rozpatrujący sprawę w I instancji. SA w Warszawie nie tylko ją pominął, ale z faktu niezgod-

[32] Powstaje ciekawy problem, w jakim zakresie okoliczność ta wpływa na wzajemną odpowiedzialność powodów (pomijając fakt, że z treści orzeczenia wynika, iż powodowie zawarli ugodę (wyr. SA w Warszawie z 8.10.2021 r., VII Aga 228/20). Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022)). Zagadnienie to wykracza jednak poza ramy niniejszego artykułu.

[33] Ustawa z dnia 29.08.1997 r. – Prawo bankowe (Dz. U. 2022 poz. 1634 ze zm.; dalej: pb).

[34] Niektórzy autorzy wskazują, że w związku z istotą umowy rachunku bankowego chodzić tu będzie przede wszystkim o bezpieczeństwo w rozumieniu art. 8 pb (utrzymywanie płynności płatniczej dostosowanej do rozmiarów i rodzaju prowadzonej działalności), zagwarantowane przepisami o charakterze publicznoprawnym, których przestrzeganie egzekwuje nadzór bankowy (Rogoń, 2005, komentarz do art. 50, pkt 6). Inni stwierdzają, że raczej należałoby uznać, iż bezpieczeństwo, o jakim mowa w komentowanym przepisie, odnosi się głównie do zapewnienia, że środki konkretnego posiadacza znajdujące się na rachunku bankowym nie zostaną wypłacone osobie nieuprawnionej (Kawulski, 2013, komentarz do art. 50, pkt 7).

[35] Warto odnotować nieco uproszczoną formułę treści art. 50 ust. 2 pb, która odwołuje się do „bezpieczeństwa przechowywanych środków pieniężnych" (podobnie art. 725 k.c.). Tymczasem, posiadacz rachunku nie jest właścicielem środków, lecz przysługuje mu wierzytelność o zwrot w gotówce lub postaci dokonania rozliczenia bezgotówkowego (podobnie Czech, 2019, s. 51, przypis 10 i 11). Nie jest natomiast oczywiste, że wierzytelność o dokonanie rozliczenia pieniężnego ma charakter pieniężny (Pyzioł, 2011, rozdział VIII, § 45, pkt II, nb. 55; Jaroch, 2016, s. 70).

[36] Przyjmuję, że taka transakcja została autoryzowana, tj. płatnik wyraził zgodę na jej wykonanie w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Nie zmienia to faktu, że z pespektywy płatnika podany w zleceniu płatniczym unikatowy identyfikator (zazwyczaj numer rachunku płatniczego) odbiorcy nie był tym, na który zgodnie z jego intencjami miały trafić środki, co jednak nie oznacza, że mamy tu automatycznie do czynienia z wadą oświadczenia woli. Przyjęcie innego poglądu oznaczałoby, że każda tego rodzaju transakcja płatnicza jest nieautoryzowana i w zasadzie brakuje stanów faktycznych, w których doszło do wykonania autoryzowanej transakcji płatniczej z podaniem przez płatnika nieprawidłowego unikatowego identyfikatora, do której zastosowanie znajduje art. 143 ust. 1 w zw. z ust. 2 zd. 1 uup. Mając na uwadze treść motywu 88 i art. 88 PSD2, byłoby to sprzeczne z intencjami prawodawcy unijnego.

[37] Podobnie wyr. SR dla Łodzi-Widzewa w Łodzi z 20.01.2021 r., VIII C 1370/19; wyr. SR dla Łodzi-Widzewa w Łodzi z 22.01.2021 r. oraz wyr. SR dla Łodzi-Widzewa w Łodzi, z 24.02.2022 r., VIIII C 979/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

ności danych odbiorcy z numerem rachunku wywiódł brak należytej staranności dostawcy, co przyjmując, że do wykonywanej transakcji zastosowanie znajdowały przepisy uup, należy ocenić jako sprzeczne z tymi przepisami. Skoro nie wymagają one od dostawcy weryfikacji zgodności danych odbiorcy z numerem rachunku (unikatowym identyfikatorem), to z braku przeprowadzenia przez dostawcę takiej czynności nie można wywodzić jego nienależytej staranności.

Pomijając kwestię niezgodności danych odbiorcy z samym numerem rachunku (z unikatowym identyfikatorem), uznanie przez sąd, że wypłata środków nastąpiła z naruszeniem standardów staranności zawodowej wymaganej od banku, jako podmiotu, który ma obowiązek szczególnej dbałości o bezpieczeństwo powierzonych mu środków pieniężnych (art. 355 § 1 i 2 k.c.), umożliwiła sądowi przypisanie bankowi odpowiedzialności odszkodowawczej deliktowej, o której mowa w art. 415 k.c.[38]. Oznacza to, że sąd przyjął, że zaistniała tzw. bezprawność bezwzględna, rozumiana jako naruszenie obowiązków o charakterze powszechnym, wynikających z przepisów prawa lub zasad współżycia społecznego (Pisuliński, 2017, s. 1040). Jest to niezwykle ważne, gdyż powodowie, w tym usługobiorca, który zainicjował transakcję, nie byli z pozwanym bankiem związani żadną relacją umowną, co wykluczało odpowiedzialność kontraktową tego banku. Z kolei odpowiedzialność kontraktowa dostawcy (banku), którego klientem był usługobiorca wyłączona była na podstawie art. 143 ust. 1 i ust. 2 zd. 1 uup (przyjmując, że transakcja miała charakter autoryzowany), co prawdopodobnie było przyczyną pozwania banku prowadzącego rachunek odbiorcy. W kontekście analizowanego orzeczenia warto zwrócić uwagę, że obecnie uppp[39] nakłada na dostawców, w tym banki, obowiązek stosowania środków bezpieczeństwa finansowego również w odniesieniu do klientów, z którymi utrzymują stosunki gospodarcze[40] oraz obowiązek bieżącego monitorowania stosunków gospodarczych klienta, w tym analizę transakcji przeprowadzanych w ramach stosunków gospodarczych[41]. Ponadto przepisy tej ustawy[42], jak również pb[43] przewidują podstawy do niewykonania transakcji lub blokady rachunku. Idąc tokiem rozumowania SA w Warszawie, mogłoby się okazać, że naruszenie tych przepisów może być rozważane jako podstawa odpowiedzialności deliktowej dostawcy wobec użytkowników usług płatniczych lub innych podmiotów, którzy nie są z tym dostawcą związani żadną umową (z zastrzeżeniem, że wysokość tej odpowiedzialności zostanie obniżona, uwzględniając stopień przyczynienia się do szkody przez te podmioty). Z treści analizowanego orzeczenia wynika, że sąd I instancji odwoływał się do nieobowiązującej już obecnie uppp2000[44], która uchylona została na mocy uppp. Niemniej SA w Warszawie rozstrzygnął sprawę, nie odwołując się do obowiązków wynikających z przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zarazem należy wyraźnie dodać, że wspomniane przepisy w pierwszej kolejności nakierowane są na ochronę interesu publicznego, w związku z czym przesądzenie czy i ewentualnie w jakim zakresie mogą stanowić podstawę odpowiedzialności cywilnej wymagałoby odrębnej analizy, która wykracza poza ramy niniejszego artykułu.

[38] Wyr. SA w Warszawie z 8.10.2021 r., VII Aga 228/20. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[39] Ustawa z dnia 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. 2022 poz. 593 ze zm.; dalej: uppp).

[40] Art. 35 ust. 2 uppp.

[41] Art. 34 ust. 1 pkt 4 lit a uppp.

[42] Art. 86 ust. 4 oraz art. 89 ust. 3 uppp, przy czym ten ostatni przepis zgodnie z art. 89 ust. 1 uppp nie dotyczy banków krajowych, oddziałów banków zagranicznych, oddziałów instytucji kredytowych oraz spółdzielczych kas oszczędnościowo-kredytowych. Zob. też art. 86 ust. 5, 9 i 10 oraz art. 87 uppp.

[43] Art. 106a ust. 3 pb.

[44] Ustawa z dnia 16.11.2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. 2017 poz. 1049 ze zm., dalej: uppp2000).

2. Wyrok Sądu Okręgowego w Olsztynie z 28 stycznia 2022 r., V Ga 328/21

W analizowanym orzeczeniu sąd poruszył wiele zagadnień mających istotne znaczenie dla rozstrzygania sporów dotyczących transakcji płatniczych[45]. Wyrok zapadł na tle sprawy, w której transakcja została wykonana wskutek działania szkodliwego oprogramowania typu *malware*, które w dniu zdarzenia funkcjonowało na komputerze klienta i które doprowadziło do podstawienia numeru rachunku oraz dodatkowo w odpowiednie miejsce danych odbiorcy w postaci imienia i nazwiska[46]. Zdaniem sądu, skoro autoryzacja tej transakcji została uzyskana poprzez doprowadzenie użytkownika bankowości elektronicznej podstępem[47] do autoryzacji transakcji, której *de facto* nie chciał wykonać poprzez podmianę danych faktycznych odbiorcy, to taka transakcja jest traktowana jako nieautoryzowana. Kwalifikacja taka jest uproszczona i budzi zasadnicze wątpliwości. Należy pamiętać, że instytucja podstępu uregulowana została w art. 86 w zw. z art. 88 k.c.[48]. Możliwość powołania się na podstęp wymaga zatem spełnienia określonych w tych przepisach przesłanek, co zostało przez sąd całkowicie pominięte. Ograniczył się on do stwierdzenia, że stwierdzony podstęp skutkuje nieautoryzowanym charakter transakcji. Tymczasem zgodnie z art. 86 § 2 k.c., podstęp osoby trzeciej jest jednoznaczny z podstępem strony, jeżeli ta o podstępie wiedziała i nie zawiadomiła o nim drugiej strony albo jeżeli czynność prawna była nieodpłatna. A przecież najczęściej (a w zasadzie prawie zawsze) – przynajmniej na gruncie obecnie funkcjonujących w obrocie rozwiązań technologicznych, dostawca nie będzie miał wiedzy o tym, że przestępcy w sposób podstępny wprowadzają klienta w błąd (zresztą odrębnego rozpatrzenia wymagałoby czy rzeczywiście w takim wypadku można mówić o błędzie w rozumieniu przepisów k.c.). Okoliczność, że to płatnik złożył zlecenie płatnicze i, komunikując się z dostawcą, obiektywnie wyraził zgodę na wykonanie transakcji, przemawiałaby za przyjęciem, że transakcja została przez płatnika autoryzowana (Wyżykowski, 2021, s. 44). To z kolei oznaczałoby, że w sprawie w ogóle nie znajdują zastosowania przepisy regulujące rozkład ryzyka i odpowiedzialności z tytułu nieautoryzowanych transakcji płatniczych. Zarazem jak wskazano wcześniej, przepisy uup wyłączają odpowiedzialność dostawców w przypadku wykonania transakcji z podaniem nieprawidłowego unikatowego identyfikatora[49] (Wyżykowski, 2021, s. 60). Za taką oceną stanu faktycznego zdaje się przemawiać fakt, iż jak wynika z ustalonego przez sąd rozpatrujący sprawę w pierwszej instancji stanu faktycznego, sporne transakcje były dodawane do koszyka przelewów, który umożliwiał dokonanie kilku przelewów w jednym czasie. Do koszyka został dodany cykliczny przelew należności za paliwo do zdefiniowanego odbiorcy (do którego klient rzeczywiście chciał zlecić wykonanie transakcji), dyspozycja została zaś potwierdzona SMS kodem[50]. Z drugiej strony, SO w Olsztynie w uzasadnieniu wyroku stwierdził, że jak słusznie zauważył biegły, klient otrzymał od banku (dostawcy) SMS z informacją o dodaniu nowego przelewu bez informacji ani o odbiorcy ani o kwocie, a wysłanie tej informacji miało miejsce jedynie dlatego, że numer podstawionego rachunku pojawił się po raz

[45] Wyr. SO w Olsztynie z 22.01.2022 r., V Ga 328/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[46] Ibidem.

[47] W wyr. mowa jest o „postępie", jednak należy przyjąć, że jest to literówka i sąd ma na myśli „podstęp". Do podstępnego działania osób trzecich odwołuje się również SR dla Łodzi-Widzewa w wyr. z 17.02.2021 r., VIII C 873/18 (zob. https://orzeczenia.ms.gov.pl/ (31.07.2022)), niemniej nie wywodzi z tego nieautoryzowanego charakteru transakcji, lecz brak rażąco niedbałego naruszenia przez klienta obowiązków ostrożnościowych przewidzianych w art. 42 uup. Orzeczenie to jest przedmiotem analizy w dalszej części artykułu.

[48] Ustawa z dnia 23.04.1964 r. – Kodeks cywilny (Dz. U. 2022 poz. 1360 ze zm.; dalej: k.c.).

[49] Art. 143 ust. 1 w zw. z ust. 2 zd. 1 uup. Zob. też motyw 88 oraz art. 88 PSD2.

[50] Wyr. SO w Olsztynie z 22.01.2022 r., V Ga 328/21, https://orzeczenia.ms.gov.pl/ (31.07.2022).

pierwszy w historii rachunku powoda[51]. Z treści orzeczenia nie wynika więc jasno, w jaki dokładnie sposób doszło do ustanowienia zdefiniowanego odbiorcy i autoryzacji transakcji.

W dalszej części orzeczenia sąd, kontynuując rozważania o tym czy transakcja została autoryzowana, stwierdził, że klient udowodnił iż transakcja była nieautoryzowana poprzez złożenie wniosku o biegłego, który to jednoznacznie potwierdził, iż w sprawie nie doszło do autoryzacji z uwagi na brak winy klienta[52]. Stwierdzenie to wymaga poczynienia kliku uwag. Po pierwsze, wina lub jej brak pozostaje bez znaczenia dla ustalenia czy płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób uzgodniony w umowie. Co najwyżej w konkretnych okolicznościach możliwe jest rozważenie czy istotnie złożone przez klienta oświadczenie woli nie jest dotknięte wadą, która pozwalałaby się od niego uchylić, lecz nie jest to problematyka winy płatnika. Po drugie, należy pamiętać, że biegły nie może wyręczać sądu w dokonywaniu ocen prawnych[53]. Tymczasem ocena czy transakcja ma charakter autoryzowany wymaga dokonania odpowiednich ustaleń faktycznych, a następnie ich subsumpcji pod właściwy stan prawny i biegły nie może w tym zakresie zastępować sądu.

Wobec tego, że SO w Olsztynie transakcję zakwalifikował jako nieautoryzowaną, wypowiadając się w przedmiocie wykładni art. 46 uup[54], w dalszej części odnoszę się do tych wywodów sądu, co nie zmienia podniesionych wcześniej wątpliwości co do prawidłowości takiej kwalifikacji. Jako zbyt daleko idące należy uznać twierdzenie przez SO w Olszynie, iż w razie, gdy transakcja jest nieautoryzowana, to wyłączną odpowiedzialność z tytułu jej przeprowadzenia ponosi dostawca usług płatniczych[55]. Przepisy uup i PSD2 nie dają podstaw do takiego wniosku (Wyżykowski, 2020, s. 78 i 79). Co najwyżej można rozważać czy intencją sądu nie było odwołanie się do konstrukcji wynikającej z art. 452 zd. 1 k.c., który stanowi, że jeżeli świadczenie zostało spełnione do rąk osoby nieuprawnionej do jego przyjęcia, a przyjęcie świadczenia nie zostało potwierdzone przez wierzyciela, dłużnik jest zwolniony w takim zakresie, w jakim wierzyciel ze świadczenia skorzystał. W tym ujęciu wykonanie przez dostawcę nieautoryzowanej transakcji rzeczywiście nie zmienia faktu, że klientowi w dalszym ciągu przysługuje wierzytelność o wypłatę kwoty równej kwocie wykonanej transakcji, chyba że możliwe jest przypisanie mu odpowiedzialności za wyrządzoną dostawcy szkodę (Pisuliński, 2003, s. 59 i 60; Pisuliński i Tereszkiewicz, 2020, s. 214–218). Niemniej brak wzmianki w orzeczeniu, który potwierdzałby taki tok rozumowania sądu[56]. Zarazem

[51] Ibidem.

[52] Ibidem.

[53] W wyr. z 20 stycznia 1970 r., II PR 18/69, LEX nr 6652 SN stwierdził, że: „Sąd może, a czasami powinien korzystać z pomocy opinii biegłego w zakresie wymagającym wiadomości specjalnych, lecz biegły nie może wyręczać sądu w dokonywaniu ustaleń i ocen prawnych, do czego nie jest ani powołany, ani nie może mieć kwalifikacji". Z kolei w wyr. z 1 lipca 1998 r., I PKN 203/98, LEX nr 36975, SN, że: „Opinia biegłego w sprawie rozumienia określonego przepisu prawnego nie może bowiem stanowić podstawy rozstrzygnięcia bez przeprowadzenia samodzielnej jego wykładni przez sąd, gdyż pojęcie »wiadomości specjalne« nie obejmuje wiedzy dotyczącej treści obowiązującego prawa oraz reguł jego tłumaczenia".

[54] W tym kontekście wątpliwości budzi również stwierdzenie przez sąd, że: „Fakt zarejestrowanego użycia instrumentu płatniczego, czyli – należy przyjąć – użycia instrumentu płatniczego zgodnie z procedurami i przy zastosowaniu ustalonych sposobów autoryzacji, nie oznacza, że transakcja została autoryzowana przez użytkownika" (wyr. SO w Olsztynie z 22.01.2022 r., V Ga 328/21; zob. https://orzeczenia.ms.gov.pl/ (31.07.2022)). Sąd ten w ogóle nie odniósł się do faktu, że art. 45 uup stanowi błędną implementację przepisów PSD2 (Wyżykowski, 2020).

[55] Wyr. SO w Olsztynie z 22.01.2022 r., V Ga 328/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[56] Przykładowo w wyr. SR Szczecin-Centrum w Szczecinie z 7 czerwca 2021 r., XI GC 617/20 (zob. https://orzeczenia.ms.gov.pl/ (31.07.2022)), sąd ten stwierdził, że: „Reasumując, pomimo wyłudzenia przez osobę nieuprawnioną mienia stanowiącego własność banku, nie dojdzie do powstania szkody po stronie posiadacza rachunku, gdyż bank nadal pozostanie zobowiązany do zaspokojenia jego wierzytelności w pełnej wysokości ze swoich środków. Innymi słowy, powodowi służy wierzytelność nie do sprawców nieuprawnionego wyprowadzenia środków z jego rachunku bankowego, a wobec pozwanego banku". W wyr. SR dla Łodzi-Widzewa w Łodzi, w wyr. z 17.02.2021 r., VIII C 873/18 (zob. https://orzeczenia.ms.gov.pl/ (31.07.2022)), sąd ten stwierdził, że: „W konsekwencji pomimo wyłudzenia przez osobę nieuprawnioną mienia stanowiącego własność banku, nie dojdzie do powstania szkody po stronie posiadacza rachunku, gdyż bank nadal pozostanie zobowiązany do zaspokojenia jego wierzytelności w pełnej wysokości ze swoich środków. Ochronę wierzytelności gwarantują posiadaczowi przepisy prawa cywilnego, finansowego i oparta na nich umowa z bankiem (por. postanowienie SN

należy dodać, że w sprawach, do których obecnie zastosowanie znajdują przepisy uup, stanowią one regulację szczególną (*lex specialis*), choć w doktrynie dostrzega się, że taki pogląd wcale nie jest oczywisty (Pisuliński i Tereszkiewicz, 2020, s. 208, 225–227)[57].

Dalej sąd stwierdził, że w sytuacji wystąpienia nieautoryzowanej transakcji pozwany jest z mocy przepisów zobowiązany do zwrotu pieniędzy objętych daną transakcją i w świetle przepisów PSD2 klient ma możliwość dysponowania kwotą nieautoryzowanej transakcji w okresie rozpatrywania reklamacji, a w rezultacie dopiero po wykonaniu powyższych czynności dostawca ma możliwość ustalenia potencjalnej odpowiedzialności klienta[58]. Takie podejście należy uznać jako zbyt uproszczone. Na marginesie nie jest jasne, dlaczego sąd wielokrotnie powołuje się bezpośrednio na PSD2, nie zaś na przepisy uup, które to stanowią właściwą podstawę prawną. Wracając do głównego nurtu rozważań, jeżeli przeprowadzona przez dostawcę w terminie jednego dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia płatnika, analiza całokształtu sprawy prowadzić będzie do uzasadnionej konkluzji, że transakcja ma charakter autoryzowany bądź też nieautoryzowany, lecz odpowiedzialność z tego tytułu w ocenie dostawcy ponosi płatnik, to trudno oczekiwać, że dostawca dokonywać będzie zwrotu środków (Wyżykowski, 2019, s. 114 i 115). Należy pamiętać, że choć obecnie raczej przyjmuje się deklaratywny charakter wpisu na rachunek płatniczy (Czech, 2019, s. 62–65; 2020, s. 90 i 91), to nie zmienia to faktu, że w świetle art. 4 ust. 1 ur[59], zasady rachunkowości (a ściślej zapis w księgach rachunkowych) muszą rzetelnie i jasno przedstawiać stan należności między stronami, a w rezultacie każdy wpis na rachunku musi być dokonany zgodnie z treścią ekonomiczną zaistniałych, relewantnych zdarzeń, w tym operacji gospodarczych (Czech, 2019, s. 49 i 50). Oczekiwanie od dostawcy, że dokonywać będzie na rachunku płatniczym wpisów, które nie odzwierciedlają jego własnych ustaleń i dokonanej oceny zdarzeń, rodzi pytanie o zgodność takiego działania z przepisami o rachunkowości.

Ostatecznie sąd stwierdził, że nie znalazł w działaniu klienta cech, którym można przepisać rażące niedbalstwo[60], co jak należy uznać przesądziło o zwolnieniu klienta z odpowiedzialności za sporną transakcję. Sąd wyjaśnił, że gdyby w momencie wykonywania (jak należy sądzić, sąd ma na myśli inicjowanie spornej transakcji) powód miał jasną informację, że transakcja ma być wykonana na inny rachunek odbiorcy, to kodu autoryzacyjnego z wiadomości SMS przesłanej przez dostawcę by nie wprowadził, a tym samym do autoryzacji transakcji w systemie bankowości elektronicznej by nie doszło[61]. Jak zasygnalizowano wcześniej, wobec niejasności co do przebiegu procesu autoryzacji, w tym zakresie trudno się odnieść do rozstrzygnięcia sądu.

z dnia 28.04.2016 roku, I KZP 3/16, L.)". Podobnie SR Szczecin-Centrum w Szczecinie z 7 czerwca 2021 r., XI GC 617/20, (zob. https://orzeczenia.ms.gov.pl (31.07.2022)). Przywołane orzeczenia będą przedmiotem analizy w dalszej części artykułu.

[57] Przykładowo w wyr. SR Szczecin-Centrum w Szczecinie z 7.06.2021 r., XI GC 617/20 (zob. https://orzeczenia.ms.gov.pl/ (31.07.2022)), który będzie przedmiotem analizy w dalszej części artykułu, sąd ten stwierdził, że: „Ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową. Ma to ten skutek, że równoległą podstawą odpowiedzialności banku jest ustawa z 19.08.2011 r. o usługach płatniczych (…)".

[58] Wyr. SO w Olsztynie z 22.01.2022 r., V Ga 328/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[59] Ustawa z dnia 29.09.1994 r. o rachunkowości (Dz. U. 2021 poz. 217 ze zm.; dalej: ur).

[60] Wyr. SO w Olsztynie z 22.01.2022 r., V Ga 328/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[61] Ibidem.

3. Wyrok Sądu Okręgowego w Poznaniu z 24 września 2021 r., XV Ca 378/21

Analizowane orzeczenie wydane zostało na kanwie sprawy, w której dostawca (bank), w dniach 29 i 30 czerwca 2019 r. wykonał 18 transakcji płatniczych zainicjowanych przez nieustalone osoby, oryginalną kartą kredytową klienta oraz każdorazowym bezbłędnym zatwierdzeniu numerem PIN, poza jedną płatnością zbliżeniową obejmującą kwotę 30 zł[62]. Z ustaleń sądu wynika, że do kradzieży karty kredytowej doszło w dniu 29 czerwca 2019 r. z samochodu powoda, kiedy na parkingu został on zaczepiony przez mężczyznę, który podjechał i zapytał się o drogę do szpitala[63]. Wtedy to ktoś wszedł do jego samochodu od strony kierowcy i niepostrzeżenie wyjął z portfela znajdującego się w plecaku kartę kredytową[64]. Numer PIN został natomiast pozyskany przez nieustalone osoby w trakcie robienia przez powoda zakupów w sklepie[65]. Słusznie należy ocenić stanowisko sądu, iż nie ma podstaw do skonstruowania domniemania faktycznego, iż skoro przestępcy znali PIN do karty kredytowej klienta, to oznacza, że musiał on im go udostępnić lub kod ten został ujawniony na skutek rażącego niedbalstwa klienta[66]. W ocenie sądu, taka konstrukcja byłaby możliwa tylko w sytuacji, gdyby można byłoby wykluczyć z dużą dozą prawdopodobieństwa możliwość ujawnienia numeru PIN w inny sposób, na przykład przez podejrzenie go przez osobę postronną lub ustalenie za pomocą urządzeń technicznych, tymczasem nie budzi najmniejszej wątpliwości, że takich ewentualności nie da się wykluczyć[67]. Jest to zatem podejście odmienne od prezentowanego przez niektóre sądy niemieckie, które przyjmują, że w przypadku nielegalnego użycia karty płatniczej w celu wypłaty środków z podaniem prawidłowego numeru PIN dowód *prima facie* (niem. *der Beweis des ersten Anscheins*) przemawia za tym, że płatnik z naruszeniem swoich obowiązków ostrożnościowych umieścił PIN na karcie lub przechowywał go w pobliżu karty, gdy do wypłaty wykorzystano oryginalną kartę[68] (Pisuliński, 2004, s. 403).

W rozpatrywanej sprawie sąd uznał, że co do zasady nieautoryzowane transakcje, będące przedmiotem postępowania, obciążają dostawcę, nie udowodnił on bowiem, że doszło do nich z powodu winy umyślnej lub rażącego niedbalstwa klienta[69]. W ślad za sądem I instancji, SO w Poznaniu uznał, że zgodnie z art. 45 uup, ciężar dowodu w tym zakresie został przerzucony na dostawcę instrumentu płatniczego[70]. Jakkolwiek sąd podzielił ocenę dostawcy, że dowodzenie tych okoliczności jest znacznie utrudnione, to zdaniem sądu oznacza to, iż ustawodawca świadomie przerzucił generalnie na instytucje finansowe ryzyko bezprawnego użycia instrumentów płatniczych[71]. Stwierdzenie to wymaga poczynienia dwóch uwag.

Po pierwsze, nałożenie przez prawodawcę unijnego na dostawców szczególnych ciężarów dowodowych nie zmierzało do przerzucenia na nich ryzyka (odpowiedzialności) z tytułu nieautoryzowanych transakcji płatniczych. Utrzymanie ogólnych zasad rozkładu ciężaru dowodu w przypadku

62 Wyr. SO w Poznaniu z 24.09.2021 r., XV Ca 378/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

63 Ibidem.

64 Ibidem.

65 Ibidem.

66 Ibidem.

67 Ibidem.

68 Wyr. Bundesgerichtshof (BGH) z 29 listopada 2011 r., XI ZR 370/10 –, juris. BGH nawiązał do wyr. BGH z 5.10.2004 r., XI ZR 210/03 –, juris oraz do postanowienia BGH z 6 lipca 2010 r., XI ZR 224/09 –, juris.

69 Wyr. SO w Poznaniu z 24.09.2021 r., XV Ca 378/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

70 Ibidem.

71 Ibidem.

sporów dotyczących transakcji płatniczych stawiałoby użytkowników w niezwykle trudnej sytuacji procesowej. W praktyce nie są oni bowiem w stanie pozyskać dowodów na okoliczności związane z inicjowaniem, a tym bardziej wykonywaniem transakcji. Celem prawodawcy unijnego było więc zapewnienie użytkownikom większej ochrony na etapie postępowania sądowego, aby w ten sposób zapewnić należytą realizację przepisów materialnych. Po drugie, treść art. 45 ust. 2 uup nie odzwierciedla w sposób pełny *ratio legis* przepisów PSD2 (a wcześniej PSD1), a więc nieprawidłowo implementuje prawo unijne i dzieje się tak na kilku płaszczyznach (szerzej zob. Wyżykowski, 2020, s. 79–82). Brak jednak szerszej wypowiedzi sądu w tym zakresie.

Wątpliwości budzi ostateczne rozstrzygnięcie sądu. Zdaniem SO klient nie miał możliwości stwierdzenia utraty (kradzieży) karty tylko przed dokonaniem pierwszej transakcji[72]. Jak wynika z samych z zeznań klienta, otrzymywał on po każdej transakcji powiadomienie, a zatem już po pierwszej transakcji mógł się zorientować, że nieupoważniona osoba dokonuje transakcji jego kartą[73]. Na gruncie tak ustalonego stanu faktycznego SO słusznie przyjął, że w świetle art. 46 ust. 2a pkt 1 uup, klient nie ponosi na podstawie art. 46 ust. 2 uup odpowiedzialności za pierwszą nieautoryzowaną transakcję płatniczą do wysokości równowartości w walucie polskiej 50 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji[74]. Wniosek taki opiera się na założeniu, że klient nie miał możliwości stwierdzenia utraty, kradzieży lub przywłaszczenia instrumentu płatniczego przed wykonaniem transakcji płatniczej oraz nie doprowadził do transakcji w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 uup. Dalej sąd stwierdził natomiast, że klient odpowiada do równowartości 50 euro za wszystkie poza pierwszą transakcją[75]. Oznacza to, że sąd jako podstawę odpowiedzialności przyjął art. 46 ust. 2 uup. W tym kontekście należy jednak pamiętać, że zgodnie z art. 42 ust. 1 pkt 2 uup, użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. W rozpatrywanej sprawie, klient otrzymał informację o wykonaniu pierwszej nieautoryzowanej transakcji w dniu 29 czerwca 2019 r., natomiast dokonał zgłoszenia utraty (kradzieży) karty w dniu 30 czerwca 2019 r., a więc dopiero następnego dnia, po wykonaniu pierwszej nieautoryzowanej transakcji i uzyskaniu informacji o tym fakcie od dostawcy[76]. Oczywiście dostawca nie poinformował klienta, że transakcja miała charakter nieautoryzowany, gdyż zasadniczo nie mógł mieć takiej wiedzy, natomiast klient wiedząc, że nie inicjował takiej transakcji, musiał powziąć przynajmniej podejrzenie, że może ona stanowić skutek działań przestępczych. Z treści orzeczenia wynika, że klient zobaczył, że na telefonie ma powiadomienia dotyczące transakcji dokonanych z wykorzystaniem karty kredytowej dopiero w dniu 30 czerwca 2019 r. około południa, wcześniej nie spoglądał na telefon, gdyż był zajęty przepakowywaniem się[77]. Przyjmując, jak uczynił to sąd, że po wykonaniu pierwszej transakcji klient mógł się zorientować,

[72] Ibidem.
[73] Ibidem.
[74] Ibidem.
[75] Ibidem.
[76] Ibidem.
[77] Ibidem.

że nieupoważniona osoba dokonuje transakcji jego kartą[78], winien on był zatem niezwłocznie poinformować o tej okoliczności dostawcę, zaniechanie tego obowiązku oznacza zaś, że ponosić będzie pełną odpowiedzialność z tytułu nieautoryzowanej transakcji na podstawie art. 46 ust. 3 uup. Art. 46 ust. 2 uup znajdzie zatem zastosowanie do momentu, w którym płatnik obowiązany byłby najpóźniej dokonać zgłoszenia tego faktu swojemu dostawcy (Wyżykowski, 2019, s. 105)[79]. W przypadku nieautoryzowanej transakcji wykonanej po upływie tego momentu[80], na podstawie art. 46 ust. 3 uup, poniesie on pełną odpowiedzialność z tego tytułu (Wyżykowski, 2019, s. 105). Natomiast, jeżeli dokona terminowego zgłoszenia, do transakcji wykonanych od tego momentu zastosowanie znajdzie art. 46 ust. 4 uup. Zarazem treść uzasadnienia omawianego wyroku daje asumpt do przyjęcia, że klient faktycznie dopiero 30 czerwca 2019 r. mógł się zorientować, że doszło do wykonania transakcji. Pojawia się więc pytanie, dlaczego, mimo że sąd uznał inaczej, nie dopatrzył się podstaw do zastosowania art. 46 ust. 3 w zw. z art. 42 ust. 1 pkt 2 uup.

Inna sprawa, że z treści orzeczenia wynika, że w dniach 29 i 30 czerwca 2019 r. dostawca zrealizował 18 transakcji płatniczych, w tym trzy wypłaty w bankomacie oraz 15 transakcji płatniczych w sklepach[81]. Jeżeli tego typu transakcje odbiegały od typowych transakcji inicjowanych przez klienta, należałoby oczekiwać, że choćby w świetle treści art. 2 RTS[82], systemy dostawcy w czasie rzeczywistym wykryją niestandardowy charakter transakcji lub nietypowe wzorce zachowań klienta, uniemożliwiając doprowadzenie przez przestępców do wypłaty lub transferu wszystkich środków znajdujących się na rachunku (lub jak miało to miejsce w rozpatrywanej sprawie – dostępnych w ramach limitu kredytu karty kredytowej).

4. Wyrok Sądu Okręgowego w Łodzi z 27 lipca 2021 r., XIII Ga 833/20

Analizowany wyrok zapadł na kanwie sprawy, w której doszło do podmiany przez złośliwe oprogramowanie numerów rachunków odbiorców z prawidłowych na błędne[83]. Mimo że sąd stwierdził, że transakcja została przez płatnika autoryzowana, na podstawie art. 46 uup orzekł o braku odpowiedzialności klienta. Jest to podejście błędne, jeżeli bowiem w ocenie sądu transakcja miała autoryzowany charakter, to brak było podstaw do stosowania art. 46 uup (Wyżykowski, 2021, s. 55). Jak już bowiem wskazano, przepisy uup wyłączają odpowiedzialność dostawców w przypadku wykonania transakcji z podaniem nieprawidłowego unikatowego identyfikatora[84] (Wyżykowski, 2021, s. 60).

[78] Alternatywnie można rozważać, czy od użytkowników usług płatniczych rzeczywiście należy oczekiwać, aby na bieżąco (niejako w czasie rzeczywistym) weryfikowali powiadomienia odnoszące się do transakcji płatniczych. Przyjmując taki obowiązek, brak takiej weryfikacji, mimo otrzymania informacji od dostawcy, może być rozpatrywany jako rażąco niedbałe naruszenie obowiązków ostrożnościowych przewidzianych w art. 42 uup.

[79] Podobnie w niemieckiej doktrynie stwierdza się, że jeżeli płatnik, mimo wiedzy o utracie lub kradzieży instrumentu płatniczego, nie powiadomił o tym dostawcy, ponosi pełną odpowiedzialność za wykonanie transakcji nieautoryzowanej (Hofmann, s. 62, pkt II.1).

[80] W wyr. SO we Wrocławiu z 29.07.2013 r., I C 1476/12, LEX nr 1848200, sąd stwierdził, że: „Mając na względzie fakt, że pozwana nie dokonała żadnych czynności mających na celu zawiadomienie o możliwym bezprawnym wykorzystaniu jej karty do transakcji (...), wedle Sądu, podnoszony przez nią zarzut zmierzający do wyłączenia jej odpowiedzialności za część operacji dokonywanych kartą, szczegółowo wymienionych w treści sprzeciwu, należało uznać za nieuzasadniony". Z kolei w wyr. SA w Warszawie z 30.08.2018 r., VI ACa 509/17, LEX nr 261788, w którym sąd uznał, że w sprawie zostało wykazane, że płatnik umyślnie, a co najmniej wskutek rażącego niedbalstwa, nie zgłosił niezwłocznie nieuprawnionego użycia instrumentu finansowego, a ponadto nie podjął należytych środków ostrożności w zakresie przechowywania instrumentu płatniczego i nieudostępniania go osobom trzecim, jak również w zakresie zabezpieczenia sprzętu, na którym inicjowano transakcje.

[81] Wyr. SO w Poznaniu z 24.09.2021 r., XV Ca 378/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[82] Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27.11.2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji C/2017/7782 (OJ L 69, 13.3.2018, p. 23–43; dalej: RTS).

[83] Wyr. SO w Łodzi z 27.07.2021 r., XIII Ga 833/20. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[84] Art. 143 ust. 1 w zw. z ust. 2 zd. 1 uup. Zob. też motyw 88 oraz art. 88 PSD2.

Wobec tego, że w dalszej części orzeczenia sąd stwierdził, że nie można przyjąć, że klient doprowadził do podmiany rachunków bankowych umyślnie lub na skutek rażącego niedbalstwa[85] (choć w istocie jest to zbędne w razie uznania przez sąd, że transakcja ma charakter autoryzowany), za pożądane uważam odniesienie się do argumentacji sądu w tym zakresie. Podzielić można stanowisko sądu, iż użytkownik nie zawsze może samodzielnie zidentyfikować złośliwe oprogramowanie, zwłaszcza biorąc pod uwagę, że komputer klienta w dacie zdarzenia miał zainstalowane zaktualizowane oprogramowanie antywirusowe, oraz że możliwe jest, że określony nowy rodzaj złośliwego oprogramowania nie zostanie wykryty przez oprogramowanie ochronne, w czym trudno upatrywać zaniedbania klienta[86]. Trudno się jednak zgodzić z twierdzeniem sądu, iż bez znaczenia pozostaje okoliczność czy osoba wykonująca sporne przelewy (w istocie sąd ma na myśli proces inicjacji) dokonała sprawdzenia numerów rachunków bankowych przed autoryzacją transakcji[87]. Sąd wyjaśnił, że ze względu na nieznany i niewykazany dowodowo mechanizm działania wirusa, podmiana numerów na poziomie komputera użytkownika mogła być dlań niedostrzegalna[88]. Tymczasem od użytkownika można oczekiwać, że przed autoryzacją transakcji zweryfikuje on treść zlecenia, celem potwierdzenia, że widniejący numer rachunku jest prawidłowy. Inaczej byłoby tylko w sytuacji, gdy na ekranie urządzenia, z którego inicjowana jest transakcja, podmiana numeru nie jest widoczna (na ekranie wyświetla się więc numer podany przez płatnika). Wówczas zmiana dotyczy wyłącznie informacji w oprogramowaniu, które finalnie kierowane są do dostawcy. Niemniej nawet wówczas należy pamiętać, że skoro treść narzędzia autoryzacyjnego (np. SMS, token) jasno wskazuje, jaka operacja (transakcja) ma być autoryzowana z wykorzystaniem danego kodu, to często nawet pobieżne (niewymagające szczególnych wysiłków) zapoznanie się z nią przez płatnika pozwala na wykrycie, że w przypadku braku zgodności z treścią zlecenia płatniczego (lub innej czynności) kod może zostać wykorzystany do wykonania czynności (transakcji) oszukańczej (Wyżykowski, 2020, s. 87). To właśnie brak rzetelnej weryfikacji przez klienta treści zlecenia oraz kodu autoryzującego, przed jego wykorzystaniem do autoryzacji transakcji, najczęściej stanowi rzeczywistą przyczynę wykonania przez dostawcę transakcji, której w istocie klient nie zamierzał inicjować. W rezultacie zachowanie takie co do zasady powinno być rozpatrywane jako rażąco niedbałe naruszenie obowiązków ostrożnościowych spoczywających na płatniku zgodnie z treścią art. 42 uup i słusznie rozstrzygają tak również niektóre sądy[89]. Ma to jednak kluczowe znaczenie wówczas, gdy kod podawany jest przez przestępców na fałszywej stronie podstawionej przez przestępców, którzy następnie wykorzystują go do zainicjowania transakcji w celu kradzieży środków. Wówczas, gdy klient komunikuje się bezpośrednio z dostawcą, podając kod za pośrednictwem prawdziwej bankowości elektronicznej (jak miało to miejsce w analizowanym orzeczeniu), zasadniczo transakcję zależałoby bowiem kwalifikować jako autoryzowaną.

85 Wyr. SO w Łodzi z 27.07.2021 r., XIII Ga 833/20. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

86 Ibidem.

87 Ibidem.

88 Ibidem.

89 Wyr. SO w Białymstoku z 24.08.2017 r., II Ca 426/17, LEX nr 2362112; wyr. SO w Łodzi z 27.03.2018 r., II Ca 51/18, LEX nr 2538475.

5. Wyrok Sądu Rejonowego Poznań-Stare Miasto w Poznaniu z 8 grudnia 2021 r., I C 648/20

Orzeczenie to zapadło na kanwie sprawy, w której klient banku (dostawcy) padł ofiarą tzw. *phishingu*, podając dane do logowania oraz otrzymane od dostawcy hasło SMS na stronie internetowej, do której został przekierowany wskutek użycia linku otrzymanego od przestępców[90]. Choć nie wynika to wprost z treści orzeczenia, można przypuszczać, że uważne zapoznanie się przez klienta z treścią hasła SMS pozwoliłoby na wykrycie, że służy on autoryzacji transakcji, której klient wcale nie zamierza zlecać i autoryzować. Tymczasem zdaniem sądu, klient miał prawo pozostawać w przekonaniu, że po kliknięciu w link zawarty w wiadomości otrzymanej z profilu swojego kolegi został przekierowany na autentyczną stronę banku i pozostając w pełnym przekonaniu co do bezpieczeństwa przeprowadzanych operacji, wpisał dane niezbędne do zalogowania się[91]. W ocenie sądu okoliczności te nie przemawiały za umyślnością albo rażącym niedbalstwie klienta[92]. Jak zasygnalizowano wcześniej, uważam, że zachowanie takie można rozpatrywać jako rażąco niedbałe naruszenie przez płatnika obowiązków ostrożnościowych.

6. Wyrok Sądu Rejonowego Szczecin-Centrum w Szczecinie z 7 czerwca 2021 r., XI GC 617/20

Z opisu stanu faktycznego sprawy zdaje się wynikać, że prawdopodobnie pełnomocnik klienta przekazał przestępcom kod lub kody z SMS otrzymane od dostawcy, wpisując je na podstawionej przez przestępców fałszywej stronie internetowej imitującej stronę dostawcy, wskutek czego przestępcy doprowadzili do zdefiniowania zaufanego odbiorcy[93]. W takim wypadku zainicjowanie samej transakcji przez przestępców możliwe było już bez udziału klienta (Wyżykowski, 2020, s. 84). Aczkolwiek z przedstawionego w orzeczeniu opisu wynika, iż pełnomocnik klienta kontaktował się z pracownikami dostawcy, sygnalizując swoje podejrzenia i wątpliwości związane ze sposobem logowania[94]. W trakcie jednej z rozmów konsultant miał polecić wpisanie kodu z SMS, jak należy rozumieć na potrzeby zdefiniowania zaufanego odbiorcy, mimo że pełnomocnik próbował się jedynie logować do rachunku. Przyjmując, że faktycznie mamy tu do czynienia z pracownikiem dostawcy (nie zaś z podszywającym się pod pracowników przestępcą), takie zachowanie należy ocenić jako co najmniej nietypowe. W rezultacie sąd uznał, że dostawca nie wykazał, aby klient (a ściślej rzecz ujmując pełnomocnik klienta) naruszył obowiązki, o których mowa w art. 42 uup umyślnie lub wskutek rażącego niedbalstwa[95]. Dalej sąd uzasadnił, że już w dniu zdarzenia pełnomocnik miał podejrzenia co do nieautoryzowanych transakcji z uwagi na podejrzane komunikaty i, mimo zgłoszenia tego dostawcy, nie doprowadziło to do zablokowania kwestionowanych przelewów[96]. Nawet zatem przyjmując, że ostateczne rozstrzygnięcie sądu jest słuszne (choć dobrowolne wpisanie przez pełnomocnika klienta kodu SMS w celu ustanowienia stałego odbiorcy, w sytuacji gdy nie inicjował on takiej operacji, należy oceniać jako co najmniej

[90] Wyr. SR Poznań-Stare Miasto w Poznaniu z 8.12.2021 r., I C 648/20. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[91] Ibidem.

[92] Ibidem.

[93] Wyr. SR Szczecin-Centrum w Szczecinie z 7.06.2021 r., XI GC 617/20. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[94] Ibidem.

[95] Ibidem.

[96] Ibidem.

nieroztropne), nie sposób nie odnieść się krytycznie do twierdzenia sądu, jakoby bank (dostawca) nie wywiązał się wobec płatnika z obowiązków wskazanych w art. 43 ust. 1 uup[97]. Sąd stwierdził, że dostawca nie zapewnił, by indywidualne dane uwierzytelniające nie były dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu[98]. Zdaniem sądu, gdyby zabezpieczenia transakcji elektronicznych stosowane przez dostawcę były właściwe, nie doszłoby do dokonania na rachunku powoda transakcji przez nieuprawnione do tego osoby[99]. Sąd poszedł jeszcze dalej i stwierdził, że nawet gdyby przyjąć, że komputer klienta został zawirusowany złośliwym oprogramowaniem (choć ostatecznie sąd stwierdził, że komputer nie był zawirusowany), to nawet wówczas dostawca powinien posiadać takie zabezpieczenia, które uniemożliwiają dostęp osobom nieuprawnionym, nawet jeżeli złośliwym oprogramowaniem dotknięte są jednostki komputerowe płatników – posiadaczy rachunków[100]. Podobną bądź też wręcz jednoaktową argumentację przedstawioną przez sąd można przy tym odnaleźć w wielu innych orzeczeniach (Wyżykowski, 2020, s. 76–78). Przykładem może być też niedawny wyrok SO w Warszawie z 2021 roku[101]. Ujawnia to niepokojące zjawisko kopiowania/powielania przez niektóre sądy argumentacji zawartej w innych orzeczeniach wydanych na kanwie podobnych spraw, bez poddania jej krytycznej analizie i ocenie.

Tymczasem nie można ani z faktu kradzieży środków (czy z faktu wykonania przez dostawcę nieautoryzowanej transakcji płatniczej), ani też z obecności na urządzeniu płatnika złośliwego oprogramowania lub innych przestępczych działań osób trzecich, niejako *a priori* zakładać, że winę i odpowiedzialność z tego tytułu ponosi dostawca (Wyżykowski, 2021, s. 54). Zwykle przestępcy wchodzą w posiadanie tych danych poprzez interakcję z płatnikami. Dzieje się tak w wyniku oszukańczych lub podstępnych[102] działań przestępców. W szczególności chodzi o ataki *phishingowe*, *pharmingowe*[103] lub inne schematy kradzieży z wykorzystaniem sieci Internet, a w szczególności z wykorzystaniem różnego rodzaju socjotechnik, wskutek których przestępcy wchodzą w posiadanie indywidualnych danych uwierzytelniających. Oczywiście wówczas można i należy badać czy dostawca należycie ostrzegł płatnika i czy wywiązał się ze spoczywających na nim obowiązkach informacyjnych. Należy również zbadać czy płatnik swoim zachowaniem nie naruszył w sposób rażąco niedbały obowiązków, o których mowa w art. 42 uup. Nie może być jednak mowy o tym, że „kradzież" środków stanowiła efekt niewłaściwego zaprojektowania czy też zabezpieczenia swoich systemów przez dostawców. Nie jest zresztą możliwe zaprojektowanie i stworzenie systemu całkowicie odpornego na działania przestępcze polegające na wyłudzaniu przez przestępców szczególnie chronionych danych dotyczących płatności od samych płatników. W tym sensie wyrażane przez niektóre sądy oczekiwanie, aby dostawcy niejako zabezpieczyli klientów przez własną niefrasobliwością, jest oczekiwaniem niemożliwym do realizacji. Analogicznie trudno konstruktorowi, sprzedawcy lub instalatorowi zamka do sejfu czynić zarzut

97 Ibidem.

98 Ibidem.

99 Ibidem.

100 Ibidem.

101 Wyr. SO w Warszawie z 11.08.2021 r., XXVII Ca 1352/21. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

102 Nie przesądza się, że chodzi tu o błąd czy podstęp w rozumieniu przepisów k.c.

103 W klasycznym *pharmingu* użytkownik, który zamierza skorzystać ze strony internetowej banku w celu skorzystania z bankowości internetowej, w rzeczywistości przekierowywany jest z wykorzystaniem złośliwego oprogramowania na fałszywą stronę internetową, na której podstępnie doprowadzany jest do przekazania indywidualnych danych uwierzytelniających, umożliwiających przestępcom zainicjowanie i autoryzację transakcji (Zahrte, 2013).

jego niewłaściwego zaprojektowania lub zainstalowania, gdy przestępcy otworzą sejf, używając do tego klucza lub szyfru otrzymanych od samego właściciela sejfu, nawet gdy stanie się tak z uwagi na jego zmanipulowanie przez przestępców (w szczególności jeżeli właściciel sejfu wyprzedzająco poinformowany został o konieczności ochrony klucza lub szyfru i skutkach naruszenia tego obowiązku).

7. Wyrok Sądu Rejonowego dla Łodzi-Widzewa z 17 lutego 2021 r., VIII C 873/18

Omawiane orzeczenie zapadło na kanwie sprawy, w której dostawca wykonał nieautoryzowaną transakcję płatniczą, do której doszło wskutek skutecznego przeprowadzenia ataku *phishingowego*[104]. Sąd przedstawił podobnie trudny do zaakceptowania pogląd, iż bank (dostawca) jako profesjonalny podmiot nie wywiązał się ze swoich obowiązków względem klienta, gdyż, jak wynikało z opinii powołanego w sprawie biegłego, bank wprowadził wprawdzie stosowne zabezpieczenia wymagane określoną normą (przy czym z uwagi na anonimizację orzeczenia w tym zakresie nie jest jasne, o jaką normę chodzi), ale niewątpliwie sam fakt kradzieży środków z rachunku klienta oznacza, że zabezpieczenia te nie były wystarczające i zostały przełamane przez twórców złośliwego oprogramowania i procesu kradzieży[105]. Zdaniem sądu, gdyby zabezpieczenia transakcji elektronicznych pozwanego banku były właściwe, nie doszłoby do dokonania na rachunku klienta transakcji przeprowadzonych przez nieuprawnione do tego osoby, przy czym jak wynika ze zgromadzonego w sprawie materiału dowodowego, takich przypadków jak klienta w pozwanym banku było znacznie więcej, co dodatkowo świadczy o tym, że zabezpieczenia stosowane przez pozwanego nie były właściwe[106]. W tym zakresie w pełni aktualne pozostają uwagi poczynione na tle analizy wyroku SR Szczecin-Centrum w Szczecinie z 7 czerwca 2021 r., XI GC 617/20 w pkt 6 powyżej.

Ostatecznie w związku z tym, że dla sądu w ślad za biegłym nie było jasne, w jaki sposób osoba trzecia uzyskała kod SMS przesłany z banku na numer telefonu klienta w dniu zdarzenia, jak również w ocenie sądu brak było dowodu wykazującego w sposób niebudzący wątpliwości, w jaki sposób i w jakiej dacie nastąpiło udostępnienie osobom nieuprawnionym danych do logowania, nie pozwalało to na przypisanie klientowi rażącego niedbalstwa w wykonywaniu wiążącej klienta z dostawcą umowy. Dalej sąd stwierdził, że judykatura konsekwentnie nie uznaje działania posiadacza rachunku, który udostępnia dane logowania na skutek podstępnego działania osób trzecich, za rażące niedbalstwo[107]. Podanie bowiem loginu i hasła na fałszywej stronie logowania należy uznać za dopuszczalny błąd w obliczu podmienionej strony, trudnej do zweryfikowania w pierwszym momencie[108]. Jak wskazano w pkt. 4 powyżej, zdarzają się orzeczenia sądów, które prezentują odmienne podejście. W szczególności podanie kodu autoryzującego, który przypisany jest do konkretnej transakcji, co do zasady trudno traktować jako dopuszczalny błąd.

[104] Wyr. SR dla Łodzi-Widzewa z 17.02.2021 r., VIII C 873/18. Zob. https://orzeczenia.ms.gov.pl/ (31.07.2022).

[105] Ibidem.

[106] Ibidem.

[107] Ibidem.

[108] Ibidem.

IV. Podsumowanie

Dokonany przegląd aktualnego orzecznictwa prowadzi do wniosku, że podobnie jak przed rokiem 2021 (Wyżykowski, 2020), utrzymuje się tendencja, by zwalniać klientów z odpowiedzialności za nieautoryzowane transakcje płatnicze (obciążać tą odpowiedzialnością dostawców)[109]. Polskie sądy powszechne zdają się być niezwykle „łaskawe" i przychylne dla klientów. Tymczasem nawet najlepsze zabezpieczenia systemowe nie są w stanie chronić przed transakcjami oszukańczymi, jeśli sami klienci nie zachowają ostrożności. Obowiązujące przepisy należałoby interpretować i stosować przy założeniu, że chronią one osoby rozsądne (Nieborak, 2010, s. 301)[110]. Model klienta (konsumenta) powinien więc ewoluować w stronę postrzegania go jako podmiotu świadomego, który choć nieprofesjonalny i nie zawsze racjonalny, to jednak jest świadomy złożoności otaczającego go świata i musi brać pod uwagę konsekwencje i ryzyko swoich działań (Nieborak, 2017, s. 433). W niedalekiej przyszłości należałoby się więc raczej spodziewać, a przynajmniej oczekiwać ewolucji linii orzeczniczej polskich sądów. W szczególności należy oczekiwać, że klienci z należytą starannością weryfikować będą treści składanych zleceń oraz treści kodów lub innych narzędzi wykorzystywanych do autoryzacji transakcji. To właśnie rozwaga klienta na tym etapie bardzo często pozwala udaremnić przestępczą próbę kradzieży środków. Brak takiej rozwagi, mimo prokonsumenckiego charakteru przepisów uup i PSD2, powinien być natomiast rozpatrywany jako potencjalnie stanowiący rażąco niedbałe naruszenie przez klienta obowiązków ostrożnościowych wynikających z art. 42 uup. Oczywiście finalnie każda sprawa wymaga indywidualnej analizy i oceny. To samo zachowanie jednego płatnika w danym kontekście przy uwzględnieniu konkretnych cech takiego płatnika będzie można ocenić jako rażąco niedbałe, podczas gdy w przypadku innego płatnika, z uwagi na szczególne okoliczności sprawy, taka ocena nie będzie uzasadniona. Z kolei pojawienie się nowych lub nietypowych, a więc nieznanych form kradzieży środków (ataków *phishingowych*) w konkretnych okolicznościach może stanowić argument za przyjęciem, że nieautoryzowana transakcji płatnicza nie była skutkiem rażąco niedbałego naruszenia przez płatnika jednego z obowiązków wynikających z art. 42 uup. Warto również odnotować, że w żadnym z orzeczeń sądy nie wypowiadały się przedmiocie obowiązku stosowania SCA. Wynika to z faktu, że żadna ze spornych transakcji nie została zainicjowana ani wykonana po dniu 14 września 2019 r. włącznie, od kiedy to dostawcy obowiązani byli spełniać wymogi dotyczące SCA.

Bibliografia

Bajor, B. (2017). W: B. Bajor, J. Byrski, A. Zalcewicz (red.), *Ustawa o usługach płatniczych. Komentarz* (wyd. II). Warszawa: Wolters Kluwer/LEX.

Balkowski, R. (2018). *Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady Poradnik klienta usług finansowych*. Warszawa: KNF.

[109] Zob. wyr. przeanalizowane w artykule, a także wyr. SO w Warszawie z 11.08.2021 r., XXVII Ca 1352/21, oraz wyr. SR Szczecin-Centrum w Szczecinie z 8 czerwca 2021 r., I C 926/20 (zob. https://orzeczenia.ms.gov.pl/ (31.07.2022)). Co ciekawe, w sprawie rozstrzygniętej przez SO w Warszawie, sąd rozpatrujący sprawę w I instancji przyjął rażące niedbalstwo klienta (należy przyjąć, że chodzi o rażąco niedbałe naruszenie obowiązków ostrożnościowych określonych w art. 42 uup).

[110] Autor, pisząc o koncepcji „lepszej regulacji", wieńczy swoje rozważania, przywołując twierdzenie L.C.B. Gowera, zgodnie z którym regulacja nie powinna dążyć do osiągnięcia niemożliwego celu, jakim jest ochrona głupców przed ich głupotą, ale w zamian za to jej cel nie powinien przekraczać więcej aniżeli ochronę rozsądnych ludzi przed robieniem z nich głupców.

Bodzioch, M. (2014). Nieautoryzowane transakcje płatnicze – wybrane zagadnienia i wątpliwości. *Monitor Prawa Bankowego*, (12).

Czech, T. (2020). Storno rachunku płatniczego. *Monitor Prawa Bankowego*, *4*.

Czech, T. (2019). Wpis na rachunek płatniczy. *Monitor Prawa Bankowego*, *10*.

Górnisiewicz, M., Obczyński, R. i Pstruś, M. (2014). *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną*. Warszawa: KNF.

Grabowski, M. (2016). Stosowanie silnego uwierzytelniania jako przesłanka odpowiedzialności banków i innych dostawców usług płatniczych. *Monitor Prawa Handlowego*, (3).

Hadnagy, C. i Fincher, M. (2017). *Mroczne odmęty phishingu, Nie daj się złowić*. Gliwice: Helion S.A.

Hofmann, C. (2018). Das neue Haftungsrecht im Zahlungsverkehr. *Zeitschrift für Bank- und Kapitalmarktrecht*, *18*(2), 62–69.

Jaroch, M. (2016). Potrącenie wierzytelności banku z wierzytelnością posiadacza rachunku bankowego. *Transformacje Prawa Prywatnego*, *3*.

Kawulski, A. (2013). *Prawo bankowe. Komentarz*. Warszawa: Wolters Kluwer/LEX.

Müller-Brockhausen, M. (2014). *Haftung für den Missbrauch von Zugangsdaten im Internet*. Nomos.

Nieborak, T. (2010). Koncepcja „lepszej regulacji" – założenia i instrumenty realizacji w Unii Europejskiej. *Ekonomia i Prawo*, *6*(1).

Nieborak, T. (2017). Konsument na rynku usług płatniczych w świetle koncepcji neutralności technologicznej. W: E. Rutkowska-Tomaszewska (red.), *Ochrona klienta na rynku usług finansowych w świetle aktualnych problemów i regulacji prawnych*. Warszawa: Wydawnictwo C.H. Beck.

Pisuliński, J. (2003). Kilka uwag o ustawie o elektronicznych instrumentach płatniczych. *Prawo Bankowe*, *1*(65).

Pisuliński, J. (2004). Odpowiedzialność posiadacza karty płatniczej za operacje dokonane przez osobę nieuprawnioną. W: M. Pyziak-Szafranicka (red.), *Odpowiedzialność cywilna. Księga pamiątkowa ku czci Profesora Adama Szpunara*. Kraków: Kantor Wydawniczy Zakamycze.

Pisuliński, J. (2017). Chwila wykonania zobowiązania pieniężnego w razie zapłaty bezgotówkowej – potrzeba zmiany interpretacji. W: P. Kostański, P. Podrecki, T. Targosz (red.), *Experientia docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple*. Warszawa: Wolters Kluwer.

Pisuliński, J. i Tereszkiewicz, P. (2020). Die Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge nach polnischem Recht. W: R. von Wesler (red.), *Buchgeld und Bargeld – Teil 2: Die Umsetzung der zweiten Zahlungsdiensterichtlinie in den CEE-Staaten, Bitcoin und andere Kryptowährungen, E-Geld*. Wien: Manz'sche Verlags-und Universitätsbuchhandlung.

Pyzioł, P. (2011). W: J. Panowicz-Lipska (red.), *System prawa prywatnego. Prawo zobowiązań – część szczegółowa* (t. 8). Warszawa; Wydawnictwo C.H. Beck/Legalis.

Rogoń, D. (2005). W: F. Zoll (red.), *Prawo bankowe. Komentarz. Tom I i II*. Kraków: Kantor Wydawniczy Zakamycze.

Rutkowska-Tomaszewska, E. (2021). FinTech – Conceptual and Regulatory Problems. Some Introductory Remarks. W: E. Bani, B. Pachuca-Smulska, E. Rutkowska-Tomaszewska (red.), *Public and Private Law and the Challenges of New Technologies and Digital Markets* (V. II. Legal Aspects of FinTech). Warszawa: Wydawnictwo C.H. Beck.

Rutkowska-Tomaszewska, E. (2021a). O aktualnych problemach i wyzwaniach ochrony konsumenta na rynku usług finansowych słów kilka (od redaktora prowadzącego). *internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *7*(10).

Torończak, M. (2019). Transakcje płatnicze wykonane z użyciem nieprawidłowego unikatowego identyfikatora. *Monitor Prawa Bankowego*, (11).

Wojtczak, D. (2012). *Usługi bankowe w regulacjach Unii Europejskiej*. Warszawa: Wolters Kluwer business/LEX a.

Wyżykowski, B. (2019). Odpowiedzialność za nieautoryzowane transakcje płatnicze – wybrane zagadnienia wynikające z implementacji PSD2. *internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *8*(8).

Wyżykowski, B. (2020). Przegląd aktualnego orzecznictwa w sprawach dotyczących nieautoryzowanych transakcji płatniczych. *Monitor Prawa Bankowego*, (9).

Wyżykowski, B. (2021). Odpowiedzialność za wykonanie transakcji płatniczej z podaniem nieprawidłowego unikatowego identyfikatora na gruncie ustawy o usługach płatniczych. *internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *7*(10).

Zahrte, K. (2013). Aktuelle Entwicklungen beim Pharming Neue Angriffsmethoden auf das Online-Banking. *MultiMedia und Recht*, (4), 207–209.