

Sygn. akt I AGa 176/18

WYROK W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 5 kwietnia 2019 r.

Sąd Apelacyjny w Białymstoku I Wydział Cywilny

w składzie:

Przewodniczący	:	SSA Beata Wojtasiak
Sędziowie	:	SSA Bogusław Dobrowolski (spr.) SSO del. Jacek Malinowski
Protokolant	:	Urszula Westfal

po rozpoznaniu w dniu 29 marca 2019 r. w Białymstoku

na rozprawie

sprawy z powództwa (...) **Spółki jawnej w O.**

przeciwko (...) **S.A. w W.**

o zapłatę

na skutek apelacji pozwanego

od wyroku Sądu Okręgowego w Olsztynie

z dnia 27 lipca 2018 r. sygn. akt V GC 106/18

I. oddala apelację;

II. zasądza od pozwanego na rzecz powoda kwotę 8 100 zł tytułem zwrotu kosztów procesu w instancji odwoławczej.

(...)

UZASADNIENIE

O. A. W. Sp.j. w O. wniósł o zasądzenie od pozwanego (...) S.A. w W. kwoty 72.210,12 euro z ustawowymi odsetkami od dnia 29 stycznia 2015r. do dnia zapłaty oraz z kosztami procesu.

Twierdził, że strony łączyła umowa rachunku bankowego. W dniu 15 stycznia 2015r. pozwany bank, wbrew dyspozycji powoda dokonał przelewu na rachunek bankowy o numerze (...) prowadzony dla osoby nieznannej powodowi na kwotę 113.544,99 euro. Przedstawiciel powoda skorzystał z opcji „kopiuj zlecenie”, w polu nr rachunku bankowego odbiorcy zamiast rachunku bankowego (...) sp. z o.o. w W., podstawiony został inny, nieznanym powodowi numer rachunku

bankowego. Powód zgłosił pozwanemu nieautoryzowany przelew i wniósł o zwrot całej kwoty. W toku postępowania karnego prowadzonego przez Prokuraturę Regionalną w B. powód odzyskał kwotę 41.334,87 euro. Obecnie dochodzi zwrotu pozostałej kwoty.

Pozwany (...) S.A. w W. wniósł o oddalenie powództwa oraz o zasądzenie od powoda na rzecz pozwanego zwrotu kosztów procesu. Podniósł, że sporny przelew został zlecony po poprawnym zalogowaniu w serwisie pozwanego banku numerem klienta oraz hasłem dostępu oraz zrealizowany w oparciu o szablon płatności prawidłowo aktywowany przy pomocy jednorazowego kodu aktywacyjnego pochodzącego z karty kodów przypisanej do powoda. Przedstawiciel powoda wybrał opcję „kopiuj zlecenie”, przez co w systemie został utworzony projekt nowego zlecenia przelewu środków na rachunek (...). Projekt nowego zlecenia miał status „do edycji”. Użytkownik dokonał zmiany modyfikacji treści przelewu zmieniając numer rachunku bankowego na numer (...), kwotę przelewu na kwotę 113.554,99 euro oraz zmianę pola „tytułem” wprowadzając (...). System (...) samoczynnie nie wstawił nowego rachunku beneficjenta, nowy numer rachunku został wstawiony na komputerze, z którego czynności wykonywał użytkownik. Użytkownik następnie autoryzował zlecenie za pomocą hasła jednorazowego z tokena. Zgodnie z § 4 ust.2 Regulaminu otwierania, prowadzenia i zamykania Zintegrowanego rachunku bankowego w (...) S.A. strony wyłączyły w swoich stosunkach m.in. stosowanie art. 45, 46 ust.2-5 ustawy o usługach płatniczych. Możliwość umownego wyłączenia stosowania m.in. art. 45 ustawy o usługach płatniczych w stosunku do klientów nie będących konsumentami zawiera regulacja art. 33 tej ustawy. Powód, na którym spoczywał ciężar dowodu, nie wykazał przesłanek odpowiedzialności pozwanego. Transakcja była autoryzowana przez powoda prawidłowo albowiem wszelkie aktywności następowały na komputerze, z którego użytkownik prawidłowo zalogował się do systemu bankowego. Każda czynność była dokonana z jednego adresu IP i czynności wymagające zgody użytkownika były prawidłowo autoryzowane przy pomocy tokena. Nie zaistniały żadne nieprawidłowości po stronie systemu bankowego pozwanego. Z informacji Prokuratury (...) w B. wynika, że na komputerze użytkownika, w dniach 14-15 stycznia 2015r. ujawniono złośliwe oprogramowanie powodujące podmianę numeru rachunku bankowego. Na skutek działań użytkownika komputera nastąpiła infekcja komputera, nie zostały podjęte żadne skuteczne działania w celu zapewnienia bezpieczeństwa systemów komputerowych powoda. Nie może mieć przy tym zastosowania art. 46 ust.1 ustawy o usługach płatniczych albowiem użytkownik w sposób prawidłowy i zgodny z łączącą powoda z pozwanym umową rachunku dokonał autoryzacji zlecenia płatniczego. Pozwany wskazał ponadto, iż powód nie udowodnił okoliczności, na którą się powoływał, a dotyczącą tego, że pozwany nie zapewnił bezpieczeństwa środków finansowych zgodnie z art. 50 ust.2 prawa bankowego. (...) bankowy powoda jest w pełni bezpieczny, a funkcja „kopiuj zlecenie” polega na kopiowaniu danych z wybranego zlecenia w celu przygotowania nowego zlecenia, jednak uwzględniając potrzeby przedsiębiorców dane mogą zostać zmienione przez użytkownika systemu. Powód wykonując czynność „kopiuj zlecenie” przy dochowaniu należytej staranności powinien był widzieć, jakie dane mogą być zmienione i jakie elementy powinny zostać przez niego zweryfikowane przed dokonaniem autoryzacji transakcji. Ingerencja w treść przekazywanych pozwanemu zleceń płatniczych nastąpiła przed dokonaniem autoryzacji przez powoda i miało to miejsce przed dokonaniem autoryzacji transakcji wskutek działania złośliwego oprogramowania na komputerze powoda. Zgodnie z § 99 ust.2 i 5 Regulaminu łączącego strony, odpowiedzialność za niewłaściwe funkcjonowanie tego urządzenia ponosi powód.

Sąd Okręgowy w Olsztynie wyrokiem z dnia 27 lipca 2018 r. uwzględnił powództwo w całości. Z ustaleń tego Sądu wynika, że powód był klientem pozwanego Banku i posiadał w tym banku rachunek bankowy. Powód zawarł w dniu 22.07.2010r. z pozwanym zintegrowaną umowę rachunku bankowego, na mocy której bank zobowiązał się do otwarcia i prowadzenia rachunku bankowego, do przechowywania środków pieniężnych klienta oraz do przeprowadzania na jego zlecenie rozliczeń pieniężnych a także do zapewnienia klientowi dostępu do środków pieniężnych zgromadzonych na wskazanych rachunkach za pośrednictwem urządzeń łączności przewodowej lub bezprzewodowej wykorzystywanych przez klienta a także do zapewnienia klientowi dostępu do informacji bankowej oraz do realizowania dyspozycji klienta. Zasady prowadzenia rachunku bankowego oraz dysponowania rachunkiem przez klienta określał Regulamin otwierania, prowadzenia i zamykania zintegrowanego rachunku bankowego w (...) S.A. z miesiąca marca 2014r.

Posiadacz uzyskał dostęp w ramach usług bankowości elektronicznej do swoich rachunków i korzystania z usług bankowości elektronicznej, na zasadach określonych w umowie i Regulaminie. W Regulaminie świadczenia usług bankowości elektronicznej określono m.in. zasady składania dyspozycji za pośrednictwem elektronicznych kanałów dostępu oraz bezpiecznego dostępu do systemu.

Powód został zobowiązany do należytego zabezpieczenia urządzeń i oprogramowania, którymi posługuje się w celu korzystania z usług bankowości elektronicznej poprzez stosowanie odpowiedniego oprogramowania. Regulamin stanowił również, że za niewłaściwe funkcjonowanie urządzeń w związku z aktywnością złośliwego oprogramowania zainstalowanego na tych urządzeniach odpowiedzialność ponosi klient.

W bankowości elektronicznej pozwany stosował system dwustopniowej autoryzacji dostępu do konta. (...) bankowości elektronicznej przy logowaniu wymaga podania poprawnego numeru klienta i odpowiadającego mu hasła ustalanego przez klienta, a następnie przed ostatecznym zatwierdzeniem zlecenia płatności w trybie przelewu jednorazowego, podania kodu autoryzacyjnego z karty kodów jednorazowych generowanego przez token.

Przed 15.01. 2015r. pozwany nie informował o zagrożeniach związanych z korzystaniem z bankowości elektronicznej.

Na komputerach powoda zainstalowane było oprogramowanie antywirusowe E. N. A. 4, które w dniach 14 i 15 stycznia 2015r. kilkakrotnie wykrywało i neutralizowało złośliwe oprogramowanie powodujące „podmianę” numeru rachunku bankowego.

W dniu 15.01.2015r. uprawniony do reprezentacji wspólnik powodowej spółki – (...) zalogował się do systemu transakcyjnego pozwanego banku (...) celem dokonania płatności dla firmy (...) Sp. z o.o. w W.. O godzinie 14.50 wybrał opcję „kopiuj zlecenie”, przez co w systemie został utworzony projekt nowego zlecenia przelewu środków na rachunek (...) Sp. z o.o. w W. o numerze (...). Projekt nowego zlecenia miał status „do edycji”. Użytkownik dokonał zmiany modyfikacji treści przelewu zmieniając kwotę przelewu na kwotę 113.554,99 euro oraz zmianę pola „tytułem” wprowadzając (...). Przed autoryzacją zlecenia, w niewyjaśniony sposób doszło do zmiany numeru rachunku bankowego odbiorcy na numer (...). Kwota 113.554,99 euro została przekazana na rachunek (...), który należał do T. P. założony i wykorzystywany przez K. S.. Użytkownik następnie autoryzował zlecenie za pomocą hasła jednorazowego z tokena.

W dniu 16.01. 2015r. powód stwierdził, że przekazane przez niego w dniu 15.01.2015r. środki pieniężne w kwocie 113.554,99 euro nie dotarły na rachunek odbiorcy (...) Sp. z o.o. w W.. W tym samym dniu powód zgłosił pozwanemu bankowi reklamację i żądanie zwrotu sumy, która została zaksięgowana na niewłaściwe konto.

Pozwany bank odmówił zwrotu przedmiotowej kwoty gdyż zlecenie transakcji było autoryzowane przez powoda przy pomocy tokena.

W dniu 21.01.2015r. powód złożył zawiadomienie o popełnieniu przestępstwa.

W wyniku prowadzonego śledztwa, Prokuratura (...) w B. postawiła zarzuty między innymi K. S. o to, że w dniu 15.01.2015r. działając w celu osiągnięcia korzyści majątkowej doprowadził T. W. do niekorzystnego rozporządzenia mieniem należącym do O. A. W. sp.j. w O. w kwocie 113.554,99 euro stanowiącej mienie znacznej wartości w ten sposób, że wprowadził w pamięci podręcznej komputera należącego do pokrzywdzonej spółki złośliwe oprogramowanie w postaci tzw. konia trojańskiego o nazwie (...) lub inne o podobnym działaniu, dzięki któremu po zalogowaniu się T. W. na platformie(...) pozwanego banku celem dokonania opłaty faktury VAT wystawionej przez (...) Sp. z o.o. w W. na kwotę 113.554,99 euro spowodował bez upoważnienia zmianę zapisu danych informatycznych w zakresie rachunku bankowego odbiorcy przelewu wewnętrznego, czym wprowadził T. W. w błąd co do okoliczności, że wykonany przez niego przelew został przekazany zgodnie z jego dyspozycją na rachunek kontrahenta o numerze (...) podczas, gdy w rzeczywistości w wyniku zamiany rachunku zasilił rachunek bankowy sprawcy o nr (...) w (...)

S.A., czym działał na szkodę wskazanej spółki. Zarzuty postawione zostały również innym osobom współpracującym z podejrzanym.

W toku postępowania karnego prowadzonego przez Prokuraturę Regionalną w B. powód odzyskał kwotę 41.334,87 euro, powód dochodzi więc zwrotu pozostałej kwoty.

Powyższy stan faktyczny Sąd ustalił na podstawie okoliczności bezspornych, dowodów z dokumentów, które w jego ocenie były wiarygodne. Załączone dokumenty oraz wydruki z systemu informatycznego banku wskazywały na historię logowań do konta elektronicznego w bankowości elektronicznej powoda załączone do odpowiedzi na pozew jak również informacje Prokuratury (...) w B. i dokument w postaci ekspertyzy D. W. nie były kwestionowane przez strony. Dowody z dokumentów stanowiły podstawę do poczynienia ustaleń faktycznych w sprawie, albowiem treść tych dokumentów była zgodna z wiarygodnymi zeznaniami świadków w części, w jakiej wskazywały na sekwencję zdarzeń i czynności T. W. w dniu 15.01. 2015r. oraz na ustalony mechanizm wykorzystany przez sprawców do przestępstwa oszustwa. Pomocne dla poczynienia ustaleń faktycznych były również zeznania świadka D. B.. Podobnie zostały ocenione zeznania T. W. w charakterze strony w części, w której podawał on okoliczność przelewu oraz korzystania podczas obsługi bankowości elektronicznej z aktualnych systemów antywirusowych, ponieważ zostało to następnie potwierdzone opinią D. W. przeprowadzoną w postępowaniu karnym. Powód wiarygodnie opisał szczegóły zawiadomienia odpowiednich osób o utracie środków pieniężnych z rachunku bankowego oraz braku znajomości z osobami, którym w toku śledztwa postawione zostały zarzuty.

Według Sądu Okręgowego powództwo podlegało uwzględnieniu na podstawie art. 471 k.c. oraz art. 725 k.c. W orzecznictwie dominuje restryktywne, uzasadnione jurydycznie stanowisko, stawiające bankom wysokie wymagania pod względem oceny staranności zachowań niezbędnych przy wykonywaniu ich zobowiązań

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 (t. j. Dz. U. z 2014 r., poz. 1175 ze zm.). Ustawa ta przewiduje generalną zasadę, że dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika. Zgodnie z art. 46 ust. 1 ustawy w przypadku wystąpienia nieautoryzowanej transakcji płatniczej, dostawca płatnika jest obowiązany niezwłocznie dokonać na rzecz płatnika zwrotu kwoty nieautoryzowanej transakcji płatniczej albo, w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Zobowiązanie banku jako profesjonalnego podmiotu jest determinowane poprzez ustawowe obowiązki wskazane m. in. w art. 43 ust. 1 ustawy. Zgodnie ze nim dostawca wydający instrument płatniczy jest obowiązany do zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Według art. 2 pkt. 10 ustawy, instrument płatniczy to zarówno zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego.

Sąd Okręgowy wskazał, że w świetle okoliczności bezspornych między stronami, a ustalonych w postępowaniu karnym prowadzonym przez Prokuraturę Regionalną w B., do spornej transakcji w dniu 15.01.2015r. doszło na skutek niezgodnego z prawem wpływu osób trzecich na przetwarzanie danych informatycznych przez internetowy system obsługi rachunku dostarczony przez pozwanego. Możliwe było z uwagi na nienależyte zabezpieczenie przez Bank dostarczonego powodowi systemu do internetowej obsługi rachunku bankowego. Bank nie zapewnił więc, aby uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywany przez użytkownika do złożenia zlecenia płatniczego nie był dostępny dla osób trzecich. Z wiarygodnych zeznań przedstawiciela powoda- T. W., potwierdzonych wydrukami logów z dnia 15.01.2015r., wynikało że internetowy system bankowy umożliwił podmianę przez osobę nieuprawnioną numeru rachunku bankowego odbiorcy, bez udziału użytkownika. Użytkownik, przy formułowaniu zlecenia korzystał z opcji „kopiuj zlecenie”. Jak wynika przy tym z zeznań T. W., dokonał on zmian

jedynie w polach „kwota transakcji” i „tytułem”, nie edytował on pola numeru rachunku bankowego. Nazwa odbiorcy nie została zmieniona, a celem skorzystania z opcji „kopiuj zlecenie” było wykorzystywanie przez użytkownika szablonu przelewu z danymi odbiorcy, przede wszystkim z wpisanym tam numerem jego rachunku bankowego. Zatem brak jest przesłanek do uznania, iż to sam użytkownik dokonał zmiany numeru rachunku bankowego. W postępowaniu karnym ustalono ponadto właściciela rachunku bankowego, na który został wysłany przelew, jak również dalsze losy środków pieniężnych przelanych przez powoda, a także najbardziej prawdopodobny mechanizm działania sprawców. Powyższe świadczy o tym, że powód stał się ofiarą przestępstwa oszustwa. Również sposób działania sprawców ustalony w postępowaniu karnym, przede wszystkim na podstawie opinii biegłego D. W. potwierdza okoliczność, iż podmiana numeru rachunku bankowego odbiorcy przelewu odbyła się bez udziału powoda.

W ocenie Sądu Okręgowego, nienależyte wykonanie umowy rachunku bankowego przez pozwanego polegało na dostarczeniu powodowi takiego systemu do obsługi internetowych transakcji dokonywanych na tym rachunku, który umożliwił podstawienie numeru rachunku bankowego przestępcy bez udziału powodowego użytkownika. Nie można obciążyć użytkownika odpowiedzialnością za dokonanie czynności zmierzających do autoryzacji zlecenia z nieprawidłowym numerem rachunku bankowego odbiorcy jak również uznać przyczynienia się powoda do szkody. Skorzystał on bowiem z opcji „kopiuj zlecenie” przelewu poprzednio już sformułowanego i wykorzystywanego wielokrotnie, aby nie przepisywać ponownie i nie sprawdzać kilkakrotnie wskazanego numeru. W styczniu 2015r. nie były medialnie rozpowszechniane informacje o tzw. „pfishingu” i sposobach działania przestępców próbujących uzyskać dostęp do środków pieniężnych klientów zgromadzonych na rachunkach bankowych przez bankowe systemy internetowe. Również pozwany Bank nie ostrzegał klientów przed tego typu atakami i nie uwrażliwiał na weryfikację wpisanych bądź skopiowanych numerów rachunków bankowych odbiorców przelewu. Dlatego niezasadne jest przerzucenie odpowiedzialności z pozwanego banku na powodowego użytkownika poprzez zarzut, że po skopiowaniu zlecenia, a przed autoryzacją przelewu, nie sprawdził on ponownie skopiowanego wcześniej numeru rachunku bankowego odbiorcy. Tym bardziej, że pozwany nie wykazał, że podmieniony numer rachunku bankowego odbiorcy był w ogóle widoczny dla użytkownika – T. W. podczas wykonywania transakcji, i że miał on możliwość i czas na reakcję.

Pozwany bank nie stawiał użytkownikom szczegółowych wymogów co do rodzaju oprogramowania antywirusowego. Okoliczność zaś, iż aktualne oprogramowanie antywirusowe było zainstalowane na komputerze powoda została wykazana w postępowaniu karnym opinią D. W..

Sąd Okręgowy stwierdził, że na Banku spoczywał szczególny obowiązek dbania o środki pieniężne zgromadzone na prowadzonych rachunkach bankowych. Obowiązek ten polegał między innymi na tym, aby dostarczyć klientom takie systemy służące do internetowej obsługi rachunków bankowych, które będą uniemożliwiały przestępcom dostęp do środków pieniężnych klientów banków. Opcja „kopiuj zlecenie” powinna więc umożliwiać tylko edycję pól nie związanych z numerem rachunku i nazwą odbiorcy ewentualnie wyraźnie sygnalizować klientowi dokonaną zmianę w tym polu. W sytuacji, kiedy użytkownik chciałby wprowadzić nowy rachunek bankowy odbiorcy, musiałby stworzyć nowy przelew. Jak wynika z załączonych do pozwu wydruków z bankowej strony internetowej, takie czynności w stosunku do aktualnych bankowych systemów internetowych pozwany bank przedsięwziął.

Zdaniem Sądu Okręgowego pozwany Bank nie wywiązał się z wypełnienia zobowiązań w stosunku do powoda wynikających z zawartej umowy. W szczególności nie zapewnił, by indywidualne zabezpieczenia instrumentu płatniczego rozumiane jako uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego nie były dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Gdyby zabezpieczenia transakcji elektronicznych stosowane przez pozwany Bank były właściwe, nie doszłoby do dokonania na rachunku powoda transakcji na rzecz nieuprawnionych do tego osób.

W ocenie Sądu Okręgowego alternatywną podstawą uwzględnienia powództwa w niniejszej sprawie jest art. 46 ust. 1 ustawy o usługach płatniczych. Ustawa ta statuuje podstawową zasadę, że dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika. 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. Stosownie do art. 46 ust. 1 w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku, gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. W myśl art. 45 ust. 1 ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. W niniejszej sprawie jednak, zgodnie z art. 33 ustawy, dostawca i użytkownik nie będący konsumentem wyłączyli stosowanie wskazanego uregulowania.

Pomimo powyższego, w ocenie Sądu Okręgowego, z okoliczności sprawy wynikało, że powodowy użytkownik nie autoryzował transakcji w podanym niżej znaczeniu. Transakcja płatnicza nosi przymiot autoryzowanej tylko wówczas, gdy płatnik wyrazi zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie pomiędzy płatnikiem a jego dostawcą (art. 40 ustęp 1). Użycie przez użytkownika zarejestrowanego instrumentu płatniczego nie jest wystarczające do stwierdzenia, że transakcja płatnicza została przez użytkownika autoryzowana. W sprawie brak jest innych okoliczności wskazujących na autoryzację transakcji płatniczej przez płatnika. Jednocześnie zgodnie z art. 43 pkt. 1 dostawca wydający instrument płatniczy jest obowiązany do zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Z obowiązkiem tym skorelowana jest powinność użytkownika instrumentu płatniczego do korzystania z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu.

Sąd Okręgowy wskazał także na implementowaną do porządku krajowego Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13.11. 2007 roku w sprawie usług płatniczych w ramach rynku wewnętrznego (Dz.U.UE. L 319/1). Jednym z celów tej Dyrektywy było zmniejszenie ryzyka i konsekwencji nieautoryzowanych lub nieprawidłowo wykonanych usług płatniczych z punktu widzenia użytkownika usług płatniczych, którym w przeważającej części przypadków pozostaje konsument. W preambule ustawodawca europejski zaznaczył m.in., że ocena ewentualnego zaniedbania ze strony użytkownika usług płatniczych winna uwzględnić wszystkie okoliczności. Oczywiście i stopień domniemanego zaniedbania powinien ocenić sąd zgodnie z prawem krajowym. W dokumencie przyjęto, że samo użycie instrumentu płatniczego niekoniecznie jest wystarczające do udowodnienia, że transakcja płatnicza została przez płatnika usług płatniczych autoryzowana (ust.2).

Zdaniem Sądu Okręgowego zgromadzony materiał dowodowy uzasadniał wniosek, że w dniu 15.11. 2015 r. ustalona w postępowaniu karnym osoba uzyskała bez wiedzy powoda dostęp do internetowego systemu transakcyjnego (...) i dokonała podmiany numeru rachunku bankowego odbiorcy przelewu. W konsekwencji doszło do ustanowienia nowego numeru odbiorcy, a następnie wykonania spornego przelewu na rzecz tego podmiotu. Brak było podstaw do uznania, że transakcje płatnicze z dnia 15.11.2015 roku były autoryzowane przez T. W.. Sam fakt prawidłowego logowania do systemu bankowości internetowej (...) przy użyciu prawidłowej nazwy użytkownika oraz hasła, a następnie sformułowanie zlecenia przelewu w oparciu o opcję „kopiuj zlecenie” i potwierdzenie hasłem zlecenia z podstawionym w międzyczasie przez przestępców numerem rachunku odbiorcy, nie przesądza jeszcze, że wykonana w tym dniu transakcja była autoryzowana przez powoda. Nie sposób uznać, że powód akceptował w jakikolwiek sposób dokonanie przelewu na rzecz osoby, której prokuratura postawiła zarzuty czy też, że miał zamiar przeprowadzić transakcję, której beneficjentem byłyby właśnie ten podmiot. Ponadto powód nigdy nie udostępniał żadnej osobie danych uprawniających do korzystania z internetowego systemu transakcyjnego banku, a wadliwy internetowy system obsługi rachunku umożliwił podstawienie numeru rachunku bankowego odbiorcy w sytuacji korzystania z opcji „kopiuj zlecenie”. Powód zgodnie z treścią łączącej go z pozwanym umowy, regulaminu, jak również normą art. 42 ust. 2 u.u.p. przechowywał dane związane z instrumentem płatniczym z zachowaniem należytej ostrożności. Nadto używany przez niego sprzęt komputerowy wyposażony był w legalne oprogramowanie systemowe oraz antywirusowe.

Według Sądu Okręgowego z samego faktu wykonania przelewu na rachunek odbiorcy nie można wyciągać wniosków prowadzących do uznania transakcji za autoryzowaną. Bezsprzecznie pozostaje fakt, że dokonanie tego typu operacji

wymagało autoryzacji poprzez wprowadzenie hasła z jednorazowego z tokena. Niekwestionowaną jest również okoliczność, że powód wprowadził do odpowiedniego pola w ramach witryny internetowej jego treść (hasło jednorazowe). Trudno jednak przyjąć, aby intencją T. W. pozostawało dokonanie tego typu operacji, skoro miał on zamiar opłacić stosowną fakturę tytułem przedpłaty ceny sprzedaży.

Przyjęcie odmiennej koncepcji i uznanie, że powód w istocie autoryzował tę czynność nie prowadzi jednak do automatycznego stwierdzenia, że autoryzował on również przelew na rzecz nieznannej mu osoby, tym bardziej, że brak podstaw do tego, aby stwierdzić, że podmieniony rachunek bankowy odbiorcy był w ogóle widoczny dla użytkownika i aby miał on możliwość reakcji na to zdarzenie.

Dlatego Sąd Okręgowy zasądził w całości dochodzoną przez powoda kwotę wraz z ustawowymi odsetkami za opóźnienie za okres od dnia wezwania do zapłaty (art. 481 § 1 i 2 k.c.).

O kosztach sądowych orzekł zgodnie z art. 98 k.p.c. Apelację od wyroku Sądu Okręgowego wniósł pozwany Bank, w której zarzucił naruszenie:

- 1) art. 471 k.c. przez jego zastosowanie, pomimo że nie doszło do jakiegokolwiek nienależytego wykonania umowy przez Bank, a tym bardziej takiego jej nienależytego wykonania, pomiędzy którym a szkodą w majątku powódki, zachodziłby adekwatny związek przyczynowy;
- 2) art. 46 ust. 1 ustawy o usługach płatniczych przez jego zastosowanie, podczas gdy z poczynionych ustaleń faktycznych, wynika że zlecenie przelewu z 15 stycznia 2018 r. zostało uprzednio autoryzowane przez działającego w imieniu spółki (...);
- 3) art. 130² § 1 k.p.c. przez przyjęcie sprawy do rozpoznania, pomimo uiszczenia przez powódkę nienależytej opłaty od pozwu.

Wnosił o zmianę wyroku i oddalenia powództwa oraz zasądzenia kosztów procesu za obie instancje, ewentualnie jego uchylenia i przekazanie sprawy Sądowi Okręgowemu do ponownego rozpoznania.

Powód domagał się oddalenia apelacji.

Sąd Apelacyjny zważył, co następuje:

Apelacja pozwanego nie jest zasadna.

Sąd Apelacyjny podziela ustalenia faktyczne zawarte w uzasadnieniu zaskarżonego wyroku. Ustalenia te mają oparcie w zgromadzonym w niniejszej sprawie materiale dowodowym, który został oceniony w zgodzie z zasadą zawartą w art. 233 § 1 k.p.c. Istotne jest w tym względzie, że skarżący w swym środku odwoławczym nie podniósł żadnych zarzutów związanych z gromadzeniem i oceną dowodów oraz dokonaniem ustaleń faktycznych, będących podstawą wyroku Sądu I instancji. Dlatego Sąd Apelacyjny także przyjął te ustalenia za podstawę faktyczną swego rozstrzygnięcia. Sąd Apelacyjny aprobuje również finalną ocenę prawną tych ustaleń w kontekście przepisów prawa materialnego, które mają w niniejszej sprawie zastosowanie. W konsekwencji zawarte w apelacji zarzuty dotyczące naruszenia tego prawa okazały się nieuzasadnione. Sąd Apelacyjny w pierwszej kolejności uznał za konieczne odnieść się do zarzutu naruszenia przez Sąd I instancji art. 46 ust. 1 ustawy o usługach płatniczych przez zastosowanie tego przepisu, podczas gdy, według skarżącego, z ustalonego stanu faktycznego wynika, iż zlecenie przedmiotowego zlecenia przelewu zostało uprzednio autoryzowane przez T. W. działającego w imieniu powoda. W związku z tak sformułowanym zarzutem należy przypomnieć, iż Sąd Okręgowy uznał, że samo użycie instrumentu płatniczego nie jest jeszcze wystarczające do wniosku o autoryzacji transakcji płatniczej przez płatnika. W tym kontekście stwierdził, że w dniu 15.01. 2015 r. osoba trzecia uzyskała bez wiedzy powoda dostęp do internetowego systemu transakcyjnego (...)dokonała podmiany numeru rachunku bankowego odbiorcy przelewu i w konsekwencji doszło do ustanowienia nowego numeru odbiorcy, na którego rzecz wykonano sporny przelew. Przedstawiona sekwencja zdarzeń ma istotne znaczenie dla rozstrzygnięcia

niniejszej sprawy. Powyższe należy odnieść do art. 40 ust. 1 i 2 ustawy o usługach płatniczych, zgodnie z którymi 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 może dotyczyć także kolejnych transakcji płatniczych. Zgoda powinna być udzielona przez płatnika przed wykonaniem transakcji płatniczej albo kolejnych transakcji płatniczych, chyba że płatnik i jego dostawca uzgodnili, że zgoda może zostać udzielona także po ich wykonaniu. W literaturze przedmiotu przyjmuje się, że autoryzacja jest oświadczeniem woli użytkownika-płatnika, skierowanym do jego dostawcy usług płatniczych (M. Grabowski: Komentarz do art. 40 ustawy o usługach płatniczych, sip.legalis.pl; także B. Bajor: Komentarz do art. 40 ustawy o usługach płatniczych, lex.online.wolterskluwer.pl). Z niewadliwych ustaleń Sądu I instancji wynika, iż działający w imieniu powoda T. W. wykonując przedmiotowy przelew wybrał opcję „kopiuj zlecenie” wyłącznie w odniesieniu do swego rzeczywistego kontrahenta - odbiorcy i jego konkretnego rachunku. Edytował jedynie pola związane z kwotą i tytułem przelewu, w każdym bądź razie nie doszło do modyfikacji wcześniej określonego numeru rachunku bankowego tego odbiorcy. Taki bowiem jest sens i istota powyższej opcji bankowości internetowej. Skoro później doszło do zatwierdzenia tego przelewu to oczywiste było, że w zamiarze jego autora miał on odnosić się do wybranego, konkretnego z nazwy odbiorcy, a nie zupełnie innej osoby, która na skutek nieprzewidzianej i niezamierzonej (de facto przestępczej) zmiany rachunku bankowego i wbrew woli dysponenta, stała się rzeczywistym beneficjentem takiej transakcji. Niesposób więc uznać taką autoryzację za prawidłową, wywołującą skutki prawne, o których mowa w art. 40 ust. 1 ustawy o usługach płatniczych. Zdaniem Sądu Apelacyjnego działanie powoda związane z autoryzacją przedmiotowego przelewu można ocenić też jako błąd, przewidziany w art. 83 § 1 k.c. Skoro autoryzacja jest kwalifikowana jako oświadczenie woli, które stanowi element czynności prawnej, i celem tej czynności było wywołanie określonych skutków prawnych związanych ze stosunkiem zobowiązaniowym, to powinna ona podlegać ocenie prawnej związanej z wadami oświadczeń woli. Autoryzacja dotyczy zapłaty świadczenia pieniężnego w wykonaniu zobowiązania, które w judykaturze i doktrynie uznawane jest za czynność prawną (por. R. Trzaskowski: Komentarz do art. 56 k.c., lex.wolterskluwer.pl.). Z okoliczności sprawy wynika, że T. W. dokując autoryzacji działał w błędnym, lecz usprawiedliwionym okolicznościami przekonaniu, że realizuje przelew na rzecz swego rzeczywistego kontrahenta. Błąd ten był błędem istotnym i mógł bowiem z łatwością przez pozwany Bank dostrzeżony ponieważ zarówno powód jak i rzeczywisty beneficjent przelewu mieli rachunki w tym Banku, dysponującym z pewnością środkami natychmiastowej weryfikacji obu stron tej dyspozycji. Powód w skierowanym do pozwanego piśmie z dnia 16 stycznia 2015 r. wskazał, że przedmiotowy przelew został dokonany przez niego błędnie ponieważ wadliwy okazał się rachunek odbiorcy oraz domagał się zwrotu przekazanych środków (k. 17). Pismo to należało zakwalifikować jako oświadczenie o uchyleniu się od skutków oświadczenia woli pod wpływem błędu i jego celem restytucja świadczenia. W orzecznictwie sądowym przyjmuje się, że art. 88 k.c. nie stawia żadnych innych wymagań w tym zakresie, każde zatem oświadczenie złożone na piśmie i wyrażające jasno wolę uchylającego się jest wystarczające. Składający oświadczenie o uchyleniu się od skutków prawnych oświadczenia woli nie ma obowiązku używania w nim określonych słów czy formułek. Nie ma więc znaczenia, czy użyje słowa „uchylam się”, czy też posłuży się jakimkolwiek innym, jeżeli z oświadczenia wynika, że nie traktuje czynności prawnej za ważną i wiążącą go (wyrok Sądu Najwyższego z dnia 13 stycznia 2010 r., II CSK 239/09, Legalis nr 336540). Powyższe przemawia za tym, że powód uchylił się od skutków swego oświadczenia woli dotyczącego autoryzacji transakcji z dnia 15 stycznia 2015 r. W tym stanie rzeczy należy uznać, iż wskazana autoryzacja nie wywołuje skutków prawnych przewidzianych w ustawie o usługach płatniczych. W konsekwencji, na gruncie art. 46 ust. 1 tej ustawy należy przyjąć, że w przedmiotowym przypadku wystąpiła nieautoryzowana transakcja płatnicza uprawniająca płatnika do żądania od jego dostawcy zwrotu kwoty nieautoryzowanej transakcji płatniczej. Dlatego słusznie Sąd Okręgowy doszedł do wniosku, że roszczenie powoda miało oparcie w tym przepisie. Sąd Okręgowy uznał odpowiedzialność pozwanego Banku wobec powoda także na podstawie art. 471 k.c. w związku z art. 725 k.c. Stanowisko to jednak nie uwzględnia szerszego aspektu stanu prawnego, który powinien być w niniejszej sprawie wzięty po uwagę. Wskazać należy na art. 63 c ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j.: Dz. U. z 2018r., poz. 2187). Zgodnie z tym przepisem polecenie przelewu stanowi udzieloną bankowi dyspozycję dłużnika obciążenia jego rachunku określoną kwotą i uznania tą kwotą rachunku wierzyciela. Bank wykonuje dyspozycję dłużnika w sposób przewidziany w umowie rachunku bankowego. W związku z tym uregulowaniem w orzecznictwie sądowym przyjmowano, że bank, który nie sprawdził, czy podany numer rachunku dotyczy wierzyciela oznaczonego w poleceniu przelewu, działa bez zachowania należytej staranności wymaganej od profesjonalisty, do

którego jego kontrahent ma szczególne zaufanie (por. wyroki Sądu Najwyższego z dnia 19 marca 2004 r., IV CK 158/03, OSNC 2005/3/54 i z dnia 17 grudnia 2008 r., I CSK 205/08, Lex nr 471143). W związku z wejściem w życie art. 143 ustawy o usługach płatniczych w piśmiennictwie wyrażono pogląd, że zamyka on wątpliwości prawne dotyczące obowiązku banków weryfikowania podanych przez osobę zlecającą dokonanie przelewu danych odbiorcy z podanym numerem rachunku bankowego tego odbiorcy. W konsekwencji powyższe poglądy judykatury utraciły aktualność. Z drugiej jednak strony roszczenia przysługujące użytkownikowi na podstawie art. 144-146 ustawy o usługach płatniczych dotyczące odpowiedzialności za wykonanie transakcji płatniczych nie wyłączają jego dalej idących uprawnień, które mogą wynikać z umowy o usługę płatniczą lub z ogólnych przepisów prawa. Wykonanie przez dostawcę obowiązków wskazanych w tych artykułach nie oznacza, iż użytkownik nie ma prawa do innych roszczeń, w szczególności na zasadach odpowiedzialności deliktowej (art. 415 i n. k.c.) czy też kontraktowej (art. 471 i n. k.c.). (M. Grabowski: Komentarz do art. 143 i art. 147 ustawy o usługach płatniczych, jw.). Wyrażono także pogląd, iż przyjęta obecnie interpretacja, według której dostawca nie ponosi odpowiedzialności i nie ma obowiązku sprawdzania, czy występuje zgodność unikatowego identyfikatora z pozostałymi danymi, jest wprawdzie zgodna z literalnym brzmieniem przepisów omawianej ustawy, niemniej trzeba się zastanowić, czy nie narusza podstawowych, ogólnych zasad prawa zobowiązań. Konieczność zachowania należytej staranności, szczególnie w przypadku podmiotu, którego należy traktować jako profesjonalistę – w szczególności w relacjach z konsumentem – zdaje się przesądzać inaczej. Zwrócić należy też uwagę, że w ujęciu art. 147 ustawy o usługach płatniczych, niezależnie od rozwiązań przyjętych w art. 144–146 (wskazujących zakres odpowiedzialności dostawcy za niewykonanie lub nienależyte wykonanie transakcji płatniczej), użytkownik może dochodzić roszczeń odszkodowawczych na zasadach ogólnych, a więc z tytułu odpowiedzialności kontraktowej dostawcy czy z tytułu czynu niedozwolonego, jeśli w wyniku działania lub zaniechania dostawcy została wyrządzona płatnikowi szkoda, a działanie czy zaniechanie dostawcy usług płatniczych nosi znamiona czynu niedozwolonego. Odpowiedzialność odszkodowawcza oparta jest wówczas na zasadzie winy. Nie wydaje się więc tak jednoznaczne wyłączenie odpowiedzialności dostawcy wobec podania przez płatnika błędnie nieprawidłowego unikatowego identyfikatora, niezgodnego z pozostałymi danymi. W tym wypadku – mając na uwadze literalne brzmienie – nie będą miały zastosowania rozwiązania przyjęte w art. 144 ust. 1 i art. 145 ust. 1 ustawy o usługach płatniczych, natomiast nie można wyłączyć odpowiedzialności odszkodowawczej dostawcy opartej na zasadach ogólnych (B. Bajor: Komentarz do art. 143 ustawy o usługach płatniczych, jw.). W świetle powyższego wykonanie zlecenia płatniczego zgodnie z treścią art. 143 ustawy o usługach płatniczych nie przesądza jeszcze o braku odpowiedzialności dostawcy płatnika, jeżeli uzasadnione okażą się w stosunku do tego dostawcy zarzuty naruszenia obowiązków wynikających z tej ustawy bądź umowy. Sąd Okręgowy trafnie wskazał w tym względzie na obowiązek Banku wynikający z art. 43 ust. 1 ustawy dotyczący zapewnienia, że indywidualne dane uwierzytelniające nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Z niewadliwych ustaleń tego Sądu wynika natomiast, że Bank nie zapewnił aby uzgodniony między stronami zbiór procedur, składających się na instrument płatniczy, nie był dostępny dla osób trzecich. Stanowiło to nienależyte wykonanie umowy rachunku bankowego ponieważ dostarczony został powodowi system obsługi internetowej transakcji, stanowiący instrument płatniczy, umożliwiający podstawienie numeru rachunku bankowego przez osobę trzecią, bez udziału użytkownika. Zgodzić się także należy z Sądem Okręgowym, że pozwany Bank nie stawiał użytkownikom szczegółowych wymogów co do rodzaju oprogramowania antywirusowego. W ustaleń tego Sądu wynikało, iż w komputerze powoda było zainstalowane aktualne takie oprogramowanie. W związku z tym nieskuteczne było powoływanie się przez pozwanego na postanowienia § 95 ust. 3 i § 100 Regulaminu otwierania, prowadzenia i zamykania zintegrowanego rachunku bankowego (k. 108) dotyczące ponoszenia przez klienta odpowiedzialności za niewłaściwe funkcjonowanie urządzenia w związku z aktywnością złośliwego oprogramowania. Stwierdzić należy, iż to przede wszystkim dostarczony instrument płatniczy umożliwiał podmianę rachunku bankowego odbiorcy w ramach opcji „kopiuj zlecenie”. Zatem to możliwość zmiany działania tego instrumentu przez osobę trzecią była przyczyną poniesionej przez powoda szkody. Zdaniem Sądu Apelacyjnego powoływane przez pozwanego postanowienia Regulaminu nie mogą doprowadzić do wyłączenia odpowiedzialności Banku związanej z nienależytym wykonaniem zobowiązania w zakresie realizacji obowiązku wynikającego z art. 43 ust. 1 ustawy o usługach płatniczych. W przeciwnym razie przewidziany w tym przepisie wymóg byłby iluzoryczny w stosunku do klienta, korzystającego z aktualnego oprogramowania antywirusowego. W ramach odpowiedzialności kontraktowej pozwanego uwzględnić także należy wskazaną wyżej kwestię zaniechania sprawdzenia czy podany przez powoda numer rachunku dotyczy wierzyciela oznaczonego w

poleceniu przelewu. Zdaniem Sądu Apelacyjnego zaniechanie to jest jednak przejawem braku należytej staranności, tym bardziej iż dysponent jak i beneficjent przelewu posiadali rachunki w tym samym banku. Z powyższych względów Sąd Apelacyjny uznał, że zarzut naruszenia przez Sąd I instancji art. 471 k.c. nie mógł zostać uwzględniony. Materiał dowodowy zgromadzony w sprawie wskazywał na wystąpienie wszystkich przesłanek odpowiedzialności kontraktowej pozwanego.

W konkluzji należy stwierdzić, że przedstawione argumenty pozostają w zgodzie z dyrektywą 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (...), mającej na celu zmniejszenie ryzyka i konsekwencji nieautoryzowanych i nieprawidłowo wykonanych usług płatniczych. Na ten aspekt niniejszej sprawy trafnie zwrócił uwagę Sąd Okręgowy w uzasadnieniu swego rozstrzygnięcia. Sąd Apelacyjny uznał, że przemawia to za korzystną dla powoda wykładnią powołanych wyżej przepisów ustawy o usługach płatniczych, która jest transpozycją wskazanej dyrektywy. Nie mógł odnieść zamierzonego przez skarżącego skutku zarzut naruszenia przez Sąd I instancji art. 130² § 1 k.p.c. Nadanie niniejszej sprawie dalszego biegu i jej merytoryczne rozpoznanie spowodowało, że kwestia nienależytej opłaty od pozwu nie może być podstawą do podważania zasadności zaskarżonego wyroku. Sąd Apelacyjny uznał, że apelacja pozwanego nie zawiera uzasadnionych podstaw. Dlatego została ona oddalona na mocy art. 385 k.p.c. O kosztach procesu w instancji odwoławczej postanowiono zgodnie z art. 98 i 108 § 1 k.p.c. oraz § 2 pkt 7 i § 10 ust. 1 pkt. 2 rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności radców prawnych (Dz. U. z 2018, poz. 265).

(...)