Sygn. akt I ACa 228/19

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 3 października 2019 r.

Sąd Apelacyjny w Białymstoku I Wydział Cywilny

w składzie:

Przewodniczący	:	SSA Jarosław Marek Kamiński (spr.)
Sędziowie	:	SA Elżbieta Bieńkowska SA Bogusław Suter
Protokolant	:	Izabela Lach

po rozpoznaniu w dniu 3 października 2019 r. w Białymstoku

na rozprawie

sprawy z powództwa ***P. D. i I. D.***

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

o zapłatę

na skutek apelacji pozwanego

od wyroku Sądu Okręgowego w Olsztynie

z dnia 21 grudnia 2018 r. sygn. akt I C 55/18

I. ***oddala apelację;***

II. ***zasądza od pozwanego solidarnie na rzecz powodów kwotę 4050 złotych tytułem zwrotu kosztów procesu instancji odwoławczej.***

(...)

UZASADNIENIE

Powodowie I. D. i P. D. wnieśli o zasądzenie na ich rzecz solidarnie od pozwanego (...) Banku (...) S.A. z siedzibą w W. kwoty 97.210 zł wraz z ustawowymi odsetkami za opóźnienie od dnia 26 września 2016 r. do dnia zapłaty. Domagali się także zasądzenia od pozwanego na ich rzecz solidarnie kosztów postępowania, w tym kosztów zastępstwa procesowego według norm przepisanych. Twierdzili, że na skutek przełamania zabezpieczeń bankowych pozwanego, padli ofiarą ataku hackerskiego, w wyniku którego dokonano nieautoryzowanych przez powodów transakcji płatniczych, obciążających ich rachunek.

Pozwany wniósł o oddalenie powództwa w całości oraz o zasądzenie kosztów zastępstwa procesowego według norm przepisanych.

Wyrokiem z dnia 21 grudnia 2018 r. Sąd Okręgowy w Olsztynie zasądził od pozwanego solidarnie na rzecz powodów kwotę 97.210 zł z odsetkami ustawowymi za opóźnienie od dnia 26 września 2016 r. do dnia zapłaty (pkt I) i zasądził od pozwanego solidarnie na rzecz powodów kwotę po 6.417 zł tytułem zwrotu kosztów procesu, w tym kwotę 5.417 zł tytułem zwrotu kosztów zastępstwa procesowego (pkt. II).

Orzeczenie to oparto o następujące ustalenia faktyczne i ocenę prawną:

W dniu 5 lutego 2014 r. I. D. i P. D. zawarli z (...) Bankiem (...) S.A. w W. umowę rachunku oszczędnościowo-rozliczeniowego (...) za zero", usług bankowości elektronicznej oraz karty debetowej (bez (...)). W ramach tej umowy, bank otworzył dla nich rachunek oszczędnościowo-rozliczeniowy (tzw. (...)) o nr (...) oraz rachunek oszczędnościowy o nr (...). Przy zawieraniu umowy klientom udzielono informacji, jak korzystać i wykonywać operacje bankowe za pośrednictwem elektronicznego sytemu bankowego. Natomiast nie udzielono im szczegółowych pouczeń, co do sprzętu, za pomocą którego mogli ich dokonywać, w tym jego zabezpieczenia, konserwacji oraz potencjalnych niebezpieczeństw, tj. ataków hackerskich. P. D. jedynie ogólnie wiedział, że musi zwracać uwagę na poziom bezpieczeństwa strony internetowej banku, na której miał się logować. Powyższe oznaczało, że strona taka winna być wyposażona w zieloną kłódkę i prefiks witryny „https". Pierwsze potwierdza, że strona posiada sprawdzony i ważny certyfikat; natomiast drugie, że jest ona szyfrowana. Te dwa elementy oznaczały, że połącznie ze stroną internetową (...) Banku (...) S.A. w W. jest bezpieczne i można na niej dokonywać operacji bankowych. Narzędziem, które małżonkowie D. wybrali do autoryzacji obsługi konta i zabezpieczające wykonywane przez nich operacje bankowych, była karta kodów kreskowych, czyli kodów numerycznych z tzw. „zdrapki". Natomiast, jeśli chodzi o login i hasło do logowania na stronę internetową banku, znali je jedynie powodowie.

W małżeństwie D. bankowością internatową, tj. wykonywaniem operacji i przelewów od 2010 r. – w ramach innych rachunków bankowych – zajmował się jedynie P. D.. Zawsze chwalił sobie ten rodzaj usług bankowych i nigdy nie miał z nimi żadnych problemów. Jeśli natomiast chodzi o jego małżonkę, to I. D. używała zazwyczaj jedynie karty płatniczej przypisanej do tych rachunków, celem dokonywania płatności po zrobieniu przez nią zakupów. Przy korzystaniu z usług bankowości elektronicznych P. D. używał jedynie swojego prywatnego laptopa marki M. o nr seryjnym (...). Laptop ten wygrał na konkursie przeprowadzonym przez (...) dla nauczycieli. Serwisował go regularnie w serwisie komputerowym (...) w O..

W czwartek 22 września 2016 r. powód próbował zalogować się na swoje konto w serwisie internetowym (...) Banku (...) S.A w W., celem wykonania przelewu na rzecz kościoła tytułem wyjazdu na tzw. rekolekcje dłuższe. Jak zawsze upewnił się, że połączenie jest bezpieczne (zielona kłódka + element „https") i podając login i hasło oraz przepisując treść znajdującą się w okienku z obrazkiem, skutecznie zalogował się na swoje konto. Po zalogowaniu mógł swobodnie poruszać się po serwisie internetowym, widział ostatnio dokonywane przez siebie operacje oraz stany swoich rachunków. Nic w działaniu strony ani jej wyglądzie nie budziło jego niepokoju. Chwilę po zalogowaniu, na monitorze wyświetlił mu się komunikat, że z powodu „przebudowy" strony musi on podać kod nr 21 z karty zdrapki, albowiem w przeciwnym razie wykonanie przelewów w ciągu najbliższych 7 dni zostanie przez bank zablokowane. Komunikatu tego nie można było wyłączyć. Powód będąc w przekonaniu, że skoro poprawnie się zalogował i widzi stan rachunków oraz historię dokonywanych przez siebie przelewów jest na prawidłowej stronie banku, podał żądany kod. Po krótkim czasie strona się zawiesiła i nie można było na niej zrobić żadnej operacji. Pojawił się komunikat, że dostęp do serwisu jest czasowo niemożliwy. Wobec powyższego, P. D. wylogował się ze strony banku. Powyższe nie wzbudziło w nim niepokoju. Stwierdził, bowiem, że skoro strona jest „w przebudowie", to nastąpiła przerwa w dokonywaniu usług bankowych.

Kilka dni przed powyższą próbą wejścia na swoje konto bankowe, P. D. na skrzynkę mailową otrzymał wiadomość e-mail, z informacją o otrzymaniu paczki. Po wejściu w wiadomość okazało się, że firma kurierska wzywała go do

odbioru paczki, której nie zamawiał. Powyższe nie wzbudziło w nim żadnego podejrzenia. Stwierdził on bowiem, że prawdopodobnie doszło do zwykłej pomyłki.

W dniach 23-26 września 2016 r. w wyniku działań przestępczych o charakterze hackerskim, na ww. rachunkach powodów nastąpiły serie nieautoryzowanych przez nich standardowych przelewów E. oraz szybkich przelewów (...). Najpierw w dniu 23 września 2016 r. z rachunku oszczędnościowego powodów przelano na ich rachunek (...) kwotę 60.000 zł i tego samego dnia wytransferowano „na zewnątrz" kwotę 57.190 zł, wykorzystując trzy przelewy na kwoty 18.410 zł, 19.290 zł i 19.490 zł. Następnie w dniu 26 września 2016 r. z tego samego rachunku oszczędnościowego przelano na rachunek (...) kwotę 50.000 zł i tego samego dnia wytransferowano również „na zewnątrz" kwotę 54.947 zł, wykorzystując trzy przelewy na kwoty 19.490 zł, 18.610 zł i 16.847 zł. Zewnętrzne wytransferowanie środków odbyło się na konto przypisane D. J. o nr (...) w Banku (...) S.A. we W., a w tytule przelewów wpisano fikcyjne oznaczenia faktur VAT. Przelewy te były dokonywane standardowym przelewem E., przez które łącznie wytransferowano z rachunków powodów kwotę 112.137 zł. Natomiast inne szybkie przelewy (...), wykonywane na rachunku powodów, zostały przez bank wychwycone i zablokowane.

W tym okresie czasu, tj. od następnego dnia po nieudanej próbie logowania do dnia 28 września 2016 r (środa) powód nie logował się na stronę banku i nie korzystał z bankowości elektronicznej. Również od dnia 17 września 2016 r. (niedziela) nie korzystał on z telefonu komórkowego, ponieważ przez przypadek zostawił go w samochodzie, którym jechał dzień wcześniej na wesele do swoich bliskich. Telefon odnalazł się dopiero w dniu 28 września 2016 r. (środa), kiedy to oddał go mu jego szwagier, który znalazł go pod siedzeniem swojego samochodu, którym wspólnie z powodem jechali na ślub. Telefon był całkowicie rozładowany. Po jego podładowaniu i uruchomieniu nie sygnalizował on jakichkolwiek prób wcześniejszych połączeń do powoda od innych osób – nie przyszły, bowiem jak zwykle żadne wiadomości – powiadomienia sms o próbie kontaktu przez kogokolwiek.

W dniu 28 września 2016 r. (czwartek) telefonicznie najpierw z powódką, a następnie czterokrotnie z powodem skontaktowali się pracownicy pozwanego z (...) Banku (...) S.A. w W.. W trakcie rozmów wyjaśniali, że dzwonią w celu potwierdzenia (autoryzowania), – choć tak naprawdę w celu weryfikacji – przelewów na znaczne kwoty, które mają być realizowane z konta powodów na konto D. J.. P. D. odmówił ich potwierdzeń oraz zażądał zablokowania konta. Pracownicy banku prosili go o niekorzystanie z karty kodów numerycznych ze zdrapki. W trakcie dalszej rozmowy jeden z pracowników banku zasugerował, że być może P. D. otwierał maile z jakimiś podejrzanymi wiadomościami i dołączonymi do nich załącznikami. Po zastanowieniu powód przyznał, że otrzymał jednego maila z informacją od kuriera o odbiorze paczki. Jednakże podał, że wiadomość ta nie była skierowana do niego, albowiem nie zamawiał żadnej paczki. Wskazał, że wówczas wiadomość ta nie wzbudzała w nim niepokoju, albowiem stwierdził on, że była to zwykła pomyłka. Pracownik banku zasugerował, żeby powód sprawdził, czy na jego komputerze nie ma wirusa i jeśli go znajdzie, żeby oddał go do serwisu celem reinstalacji i przeformatowania dysku. Podczas tych rozmów żaden z pracowników banku nie poinformował powodów o zaborze środków z ich rachunku bankowego – mimo wiedzy o tym już w tamtej chwili. W związku z tym powodowie uznali, że doszło jedynie do próby włamania się na ich rachunek bankowy, natomiast zablokowanie konta oraz karty kodów w pełni zabezpieczy środki pieniężne na nim się znajdujące. Uznając, że sprawa jest zakończona, nie dokonali sprawdzenia stanu swoich rachunków na koncie bankowym.

W następnym dniu, tj. 29 września 2016 r. P. D., zgodnie z sugestiami pracownika pozwanego, zaniósł sprzęt do serwisu celem reinstalacji systemu operacyjnego. Powyższe zatarło wiele informacji z działań dokonywanych na tym laptopie, co uniemożliwiło rozstrzygnięcie, czy komputer powoda został zawirusowany złośliwym oprogramowaniem lub oprogramowaniem wyłudzającym dane. Niemożliwym okazało się także jednoznaczne określenie, jaki system operacyjny był zainstalowany przed tą datą na laptopie powoda oraz czy był on systemem legalnym, jak też czy posiadał program antywirusowy. Z informacji, jakie zachowały się na dysku, wynikało, że był to system z rodziny W.. Nie dało się natomiast określić, jaka konkretnie wersja systemu była zainstalowana.

W dniu 29 września 2016 r. pozwany sporządził zawiadomienie o podejrzeniu popełniania przestępstwa oraz pismem z dnia 17 października 2016 r. uzupełnił to zawiadomienie. W ich treści wskazał m.in., że zidentyfikował przypadki realizacji nieuprawnionych przelewów z rachunków powodów, dokonanych jego zdaniem poprzez

prawdopodobnie zainfekowany złośliwym oprogramowaniem komputer. Powyższe informacje podał, mimo że żaden z jego pracowników nie zbadał laptopa powodów. Wskazał też, że środki te zostały początkowo zaksięgowane na rachunku należącym do D. J. i następnie wytransferowane na inne rachunki. Część środków została przetransferowana za pośrednictwem kanału B. M. na kwotę 14.927 zł na konto prowadzone przez (...) Banku (...) S.A. w W. na rzecz S. C. (1). Wobec czego, zgodnie z art. 106a ust. 3 i 4 Prawa bankowego, w dniu 17 października 2016 r. o godz. 8:00 na 72 godziny na rachunku nr (...) założył blokadę środków na kwotę 14.920,10 zł. Ponadto bank zgodnie z art. 106c ust 5 i 6 Prawa bankowego zwrócił się o wydanie postanowienia przez uprawniony organ o przedłużenie tej blokady na dalszy okres 3 miesięcy.

W dniu 3 października 2016 r. (poniedziałek) powódka I. D. udała się osobiście do Oddziału 3 (...) Banku (...) S.A. w W., aby odblokować konto bankowe. W placówce okazało się, że nie zostało ono w ogóle zablokowane, pomimo wyraźnej dyspozycji telefonicznej powoda. Dopiero podczas wizyty w banku powódka dowiedziała się, że przelewy, których P. D. telefonicznie nie autoryzował, zostały wykonane oraz że z ich rachunków zniknęły pieniądze. W związku z tym, od razu złożyła reklamację w tym przedmiocie, która to nie została przez bank uwzględniona.

Po zgłoszeniu reklamacji powód w tym samym dniu, tj. 3 października 2016 r. złożył ustne zawiadomienie o popełnieniu przestępstwa i został przesłuchany. Powódka zaś została przesłuchana w tej samej sprawie w dniu 28 listopada 2016 r.

Prokuratura Rejonowa W. Ż. w W. w dniu 17 października 2016 r. wszczęła śledztwo w sprawie o sygn. akt PR 3 Ds. (...).2016.VI, m.in. w sprawie dokonania w krótkich odstępach czasu, z góry powziętym zamiarem, w celu osiągniecia korzyści majątkowej, w okresie od 23 września 2016 r. do 28 września 2016 r. w bliżej nieustalonym miejscu nieuprawnionych transakcji za pośrednictwem sieci Internet poprzez wykonanie bezprawnych przelewów środków pieniężnych na szkodę P. D. i I. D.. Postępowanie w zakresie tego czynu następnie prowadziła Prokuratura Rejonowa w Pile, zaś obecnie Prokuratura Okręgowa w Białymstoku.

Prokurator Prokuratury Rejonowej W. Ż., mając na uwadze wniosek banku, postanowieniem z dnia 17 października 2016 r. postanowił dokonać blokady rachunku bankowego o nr (...) prowadzonego przez (...) Bank (...) S.A w W. dla S. C. (2), dotyczącą środków pieniężnych w wysokości 14.920,10 zł.

Mając na uwadze dokonane w toku postępowania przygotowawczego ustalenia, w tym zwłaszcza zeznania świadków – P. D., S. C. (2) oraz P. C., Prokurator Prokuratury Rejonowej w Pile postanowieniem z dnia 10 stycznia 2017 r. uchylił powyższą blokadę. Ponadto uznał, że zatrzymane środki pieniężne w wysokości 14.927 zł stanowią własność P. D. i I. D. i jako zbędne dla postępowania karnego przekazał na ich rachunek, prowadzony w pozwanym banku o numerze (...).

Ostatecznie powodowie w dniu 15 grudnia 2017 r. wezwali pozwany bank do zwrotu ich środków pieniężnych w kwocie 97.210 zł wraz z należnymi odsetkami od dnia 26 września 2016 r. do dnia zapłaty, pod rygorem skierowania sprawy na drogę postępowania sądowego. W piśmie z dnia 2 marca 2018 r. pozwany stwierdził, że mimo ponownej weryfikacji sprawy, nie dała ona podstaw do zmiany jego stanowiska i odmówił zwrotu żądanej kwoty.

Na stronie internetowej pozwanego banku w 2016 r. widniała informacja ostrzegawcza o zachowaniu ostrożności przy dokonywaniu bankowych czynności elektronicznych. W 2018 r. znalazły się na niej dodatkowo ostrzeżenia, że logowanie do serwisu nie wymaga podania kodu z narzędzia autoryzacyjnego. Ponadto, zamieszczono tam komunikat, żeby klient nigdy nie podawał kodu podczas logowania, ani bezpośrednio po zalogowaniu do serwisu. Jak również, żeby nie korzystać z linków do dokonania płatności przesyłanych przez osoby trzecie, a także, żeby zachować ostrożność wobec wiadomości wysyłanych np. z portali społecznościowych typu F. czy witryn ze sprzedażą typu (...), zawierających prośbę o skorzystanie z przesłanego linku w celu dokonania płatności. Linki te mogą bowiem kierować klienta na fałszywą stronę banku.

W tak ustalonym stanie faktycznym, Sąd Okręgowy uznał powództwo za uzasadnione w całości. Podał, 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 (por. wyrok Sądu Apelacyjnego w Warszawie z dnia 19 lipca 2018 r., I ACa 348/17).

Podstawę odpowiedzialności banku w tym zakresie stanowią przepisy ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2016.1572 j.t.), która przewiduje generalną zasadę, zgodnie z którą dostawca usług płatniczych (bank) ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika, czyli posiadacza konta (art. 46 ust. 1 ustawy). Ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika i prawidłowo zapisana w systemie służącym do obsługi transakcji płatniczych dostawcy oraz że nie miała na nią wpływu awaria techniczna, ani innego rodzaju usterka związana z usługą płatniczą świadczoną przez tego dostawcę, w tym dostawcę świadczącego usługę inicjowania transakcji płatniczej – spoczywa zaś na dostawcy tego użytkownika, a więc na pozwanym (art. 45 ust. 1 powołanej ustawy). Transakcję płatniczą uważa się natomiast za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą (art. 40 ust. 1 ustawy).

Mając to na uwadze, a także treść § 2 pkt 2 regulaminu świadczenia bankowości elektronicznej u pozwanego oraz zgodne stanowisko stron, co do tego, że sposobem autoryzacji wszystkich operacji na rachunku powodów była karta kodów jednorazowych, czyli kodów numerycznych z tzw. „zdrapki", Sąd Okręgowy stanął na stanowisku, że w sprawie nie było podstaw do przyjęcia, że powodowie wyrazili zgodę na wykonanie przelewów w dniach 23-26 września 2016 r. na łączną kwotę 112.137 zł, skoro stanowczo temu zaprzeczali. Pozwany nie kwestionował zresztą tej okoliczności, a nawet sam zgłosił zawiadomienie o podejrzeniu popełniania przestępstwa na rachunku powodów przez cyberprzestępców.

W efekcie Sąd uznał, że pomimo uwierzytelniania dokonanych w tych dniach transakcji (przez osobę nieuprawnioną tj. hackera) za pomocą wyłudzonych od małżonków D. instrumentów, mających identyfikować posiadacza rachunku bankowego (tj. loginu i hasła oraz jednorazowego kodu numerycznego z tzw. „zdrapki"); nie były one jednak przez powodów autoryzowane (art. 40 ust. 1 ustawy). Powód, który zajmował się bankowością elektroniczną – co przyznała powódka, a nie zaprzeczył pozwany – sam ich bowiem nie autoryzował. Poza tym, jak wskazywał świadek P. C., system bankowy pozwanego wykrył część działań powodów, tj. szybkie przelewy (...) wykonywane na rachunku powodów przez osoby trzecie i je zablokował.

W ocenie Sądu Okręgowego, pozwany nie udowodnił również, aby powodowie, jako płatnicy, umyślnie doprowadzili do nieautoryzowanej transakcji płatniczej albo umyślnie lub wskutek rażącego niedbalstwa dopuścili się naruszenia, co najmniej jednego z obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych. W sprawie nie było bowiem dowodów o przekazaniu, w trakcie zawierania przez małżonków D. umowy, jakichkolwiek informacji o sprzęcie, za pomocą którego mogli oni dokonywać operacji bankowych, w tym sposobie jego zabezpieczenia, konserwacji oraz potencjalnych zagrożeń przez tzw. „ataki hackerskie". Sąd nie miał też wątpliwości, że powód podczas logowań był zawsze ostrożny (każdorazowo zwracał uwagę na stronę internetową banku i jej zabezpieczenia – wyposażenie w zieloną kłódkę i prefiks witryny „https"). Pozwany nie wykazał natomiast, aby w dniu przedmiotowego zdarzenia hackerskiego – poza informacją ostrzegawczą o zachowaniu ostrożności przy dokonywaniu bankowych czynności elektronicznych – na jego stronie internetowej umieszczone były inne, szczegółowe informacje o zagrożeniach, w tym, że logowanie do serwisu nie wymaga podania kodu z narzędzia autoryzacyjnego; aby klient nigdy nie podawał kodu podczas logowania, ani bezpośrednio po zalogowaniu do serwisu; żeby nie korzystać z linków do dokonania płatności przesyłanych przez osoby trzecie czy aby zachować ostrożność wobec wiadomości wysyłanych, np. z portali społecznościowych czy witryn ze sprzedażą, zawierających prośbę o skorzystanie z przesłanego linku w celu dokonania płatności. Uwadze Sądu nie uszło również, że strona internetowa, z której skorzystał powód, była bliźniacza do tej właściwej. Jej szata graficzna i pojawiające się informacje były bowiem identyczne, jak te pojawiające się dotychczas podczas korzystania przez powoda z bankowości elektronicznej. Mając przy tym na uwadze treść § 10 regulaminu świadczenia usług bankowości elektronicznej pozwanego, która wskazywała, że klient mógł składać dyspozycje za pośrednictwem elektronicznych kanałów dostępu przez całą dobę z wyłączeniem okresu przerw niezbędnych do konserwacji, napraw technicznych lub przywrócenia poprawności funkcjonowania elektronicznych kanałów dostępu, a informacje o wystąpieniu przerwy były dostępne na stronie internetowej lub w serwisie

internetowym lub serwisie telefonicznym, Sąd Okręgowy przyjął, że powód mógł pozostawać w usprawiedliwionym przekonaniu, że komunikat wyświetlający się podczas logowania był prawdziwy i pochodził od pozwanego Banku. W efekcie przyjął, że wpisanie przez powoda kodu ze zdrapki, po zalogowaniu się do swojego konta, nie nosiło cech rażącego niedbalstwa.

Jednocześnie, wobec polecenia powodowi dokonania reinstalacji systemu operacyjnego przez pracowników pozwanego, za niemożliwe Sąd Okręgowy uznał udowodnienie, czy na laptopie powoda zainstalowano oprogramowanie antywirusowe, ani też czy komputer ten był zawirusowany złośliwym oprogramowaniem lub oprogramowaniem wyłudzającym dane. Niemożność weryfikacji danych znajdujących się w dniu zdarzenia na laptopie, Sąd ustalił w oparciu o opinię biegłego sądowego, którą uznał za rzetelną i konkretną. Analogicznie ocenił wykazanie, czy ewentualnie po zainstalowaniu wirus przedostał się do komputera powoda z chwilą odbioru przez niego maila o dostarczeniu mu przez kuriera paczki.

Pomijając wniosek pozwanego o przeprowadzenie dowodu z opinii biegłego na okoliczność ustalenia adresu IP komputera powoda, Sąd uznał, że okoliczności, na które wniosek ten powołano zostały już dostatecznie wyjaśnione. Poza tym, wobec treści ustnej opinii biegłego, w której wyjaśniono, że adres IP wskazywał, iż transakcje na koncie bankowym powodów wykonano z tego samego komputera, przy czym obie operacje zostały dokonane przez cyberprzestępcę bądź były działaniem bardzo złożonego wirusa – stwierdził, że okoliczności, dla których wniosek ten powołano nie miały już znaczenia dla rozstrzygnięcia sprawy.

Zdaniem Sądu, powód nie naruszył także obowiązku niezwłocznego zgłoszenia dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. Powód nie mógł bowiem podać niezwłocznie takiej informacji bankowi, skoro zaufał informacjom podanym na stronie internetowej banku, że jest ona w przebudowie. Następnie, przez kilka dni nie korzystał z bankowości internetowej, ponieważ nie miał takiej potrzeby, zaś kolejno – był poza domem (na weselu). Zważywszy zaś, że jako pierwszy o nieuprawnionym użyciu instrumentu płatniczego dowiedział się sam pozwany, a mimo czterokrotnych rozmów z powodem żaden z pracowników pozwanego nie poinformował powoda o wytransferowaniu na zewnątrz jego środków pieniężnych, Sąd uznał, że powód był zwolniony z obowiązku zawiadomienia banku, określonego w art. 42 ustawy o usługach płatniczych.

Uznając więc, że pozwany nie wykazał zaistnienia którejkolwiek z przesłanek, wyłączających jego odpowiedzialność, Sąd Okręgowy stanął na stanowisku, iż jest on zobowiązany – zgodnie z art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2016.1572 j.t.) – do niezwłocznego zwrotu powodom kwoty nieautoryzowanych transakcji płatniczych, tj. 97.210 zł (bez kwoty zwróconej im w toku postępowania przygotowawczego).

O odsetkach rozstrzygnął na podstawie art. 481 § 1 k.c.

O kosztach procesu orzekł zaś w oparciu o art. 98 § 1, 3, 4 k.p.c. w zw. z art. 99 k.p.c.

Apelację od tego wyroku wywiódł pozwany, który zaskarżył go w części i zarzucił Sądowi Okręgowemu naruszenie:

1. przepisów prawa procesowego, tj.:

- art. 233 § 1 k.p.c. poprzez dowolną ocenę materiału dowodowego, z pominięciem w ustaleniu stanu faktycznego dowodu z dokumentu w postaci wyciągu z logo systemowego, którego treść (zapisy wejść i operacji przeprowadzonych za pośrednictwem systemu elektronicznego w dniu 22 września 2016 r.) zaprzecza zeznaniom powoda, co do okoliczności, w jakich doszło do utraty kodu autoryzacji transakcji nr 21, co mogło skutkować wadliwym ustaleniem stanu faktycznego, co do utraty przez powoda narzędzia autoryzacji,

- art. 217 § 3 k.p.c. w zw. z art. 217 § 1 k.p.c. w zw. z art. 227 k.p.c. w zw. z art. 278 § 1 k.p.c. poprzez oddalenie dowodu z opinii biegłego sądowego, w przedmiocie ustalenia czy nr IP 83.6.43.157, identyfikujący komputer, należał

do komputera powoda, z którego przeprowadzono transakcje w dniu 22 września 2016 r., co pomogłoby wyjaśnić, czy kwestionowana transakcja była autoryzowana,

- art. 233 § 1 k.p.c. poprzez dowolną ocenę materiału dowodowego, co skutkowało pominięciem w ustaleniu Sądu, czy powód wywiązał się z umowy w przedmiocie oprogramowania w zakresie jego aktualizacji i legalności,

2. przepisów prawa materialnego, polegające na:

- błędnej wykładni art. 42 ust. 1 pkt 1 i 2 ustawy o usługach płatniczych poprzez przyjęcie, że zachowanie powoda, polegające na udostępnieniu kodu autoryzacji transakcji w celu innym niż autoryzacja transakcji i nie powiadomienie o tym Banku, nie stanowi rażącego niedbalstwa,

- niewłaściwym zastosowaniu art. 46 ust. 3 ustawy o usługach płatniczych poprzez przyjęcie, że Bank odpowiada za kwestionowane transakcje mimo, że były one skutkiem rażącego niedbalstwa powoda w wykonywaniu obowiązków, wynikających z umowy, jak i z przepisów art. 42 ust. 1 ustawy o usługach płatniczych.

Wskazując na tak sformułowane zarzuty, wniósł o zmianę zaskarżonego wyroku i oddalenie powództwa oraz o zasądzenie kosztów procesu, w tym kosztów zastępstwa procesowego za obie instancje; ewentualnie wniósł o uchylenie zaskarżonego wyroku i przekazanie sprawy Sądowi I instancji do ponownego rozpoznania, przy uwzględnieniu kosztów postępowania odwoławczego, w tym kosztów zastępstwa procesowego.

Domagał się nadto dopuszczenia dowodu z opinii uzupełniającej biegłego sądowego z zakresu informatyki, celem wyjaśnienia czy nr IP 83.6.43.157, identyfikujący komputer, należał do komputera powoda i czy wykorzystanie kodu autoryzacji transakcji nr 21 do utworzenia szablonu płatności nastąpiło z komputera powoda.

Powodowie wnieśli o oddalenie apelacji pozwanego, pominięcie zgłoszonego w apelacji wniosku dowodowego oraz o zasądzenie od pozwanego solidarnie na ich rzecz kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych.

Sąd Apelacyjny zważył, co następuje:

Apelacja nie była uzasadniona.

Żaden z podniesionych w niej zarzutów nie okazał się trafny. Przede wszystkim nieuzasadnione okazały się te zarzuty procesowe, w ramach których strona skarżąca kwestionuje dokonaną przez Sąd I instancji ocenę zgromadzonego w sprawie materiału dowodowego. Trzeba podkreślić, że dla skutecznego postawienia zarzutu naruszenia art. 233 § 1 k.p.c. nie jest wystarczające przekonanie strony o innej niż przyjął to sąd, wadze (doniosłości) poszczególnych dowodów i ich odmiennej ocenie niż ocena sądu. Konieczne jest bowiem wykazanie, że sąd uchybił zasadom logicznego rozumowania lub doświadczenia życiowego, gdyż tylko takie uchybienie może być przeciwstawione uprawnieniu sądu do dokonywania swobodnej oceny dowodów. Jeżeli zaś z określonego materiału dowodowego sąd wyprowadza wnioski logicznie poprawne i zgodne z doświadczeniem życiowym, to ocena sądu nie narusza reguł swobodnej oceny dowodów i musi się ostać, choćby w równym stopniu, na podstawie tego materiału dowodowego, dawało się wysnuć wnioski odmienne. Tylko w przypadku, gdy brak jest logiki w wiązaniu wniosków z zebranymi dowodami, lub gdy wnioskowanie sądu wykracza poza schematy logiki formalnej, albo wbrew zasadom doświadczenia życiowego nie uwzględnia jednoznacznych praktycznych związków przyczynowo – skutkowych, to przeprowadzona przez sąd ocena dowodów może być skutecznie podważona (por. wyrok Sądu Najwyższego z dnia 27 września 2002 r., akt IV CKN 1316/00; wyrok Sądu Najwyższego z dnia 14 stycznia 2000 r., sygn. akt I CKN 1169/99).

W niniejszej sprawie skarżący takiego wywodu nie przedstawił, poprzestając w istocie na wskazaniu jedynie własnej, subiektywnej oceny faktów ustalonych przez Sąd I instancji. Generalnie zarzuty w tym zakresie sprowadzają się do forsowania korzystnej dla pozwanego oceny stanu faktycznego; zmierzającego do wykazania, iż wyprowadzone z rachunku bankowego powodów transakcje były przez nich autoryzowane, a nadto, że zachowanie P. D., w trakcie

logowania do systemu bankowości elektronicznej pozwanego w dniu 22 września 2016 r., obarczone było rażącym niedbalstwem.

Wbrew jednak temu, co twierdzi skarżący, prawidłowo wywiódł Sąd Okręgowy, że nie zdołał on wykazać, aby transakcje, poprzez które objęte pozwem środki zostały wyprowadzone z rachunku bankowego, były autoryzowane przez płatników, czyli małżonków D.. Nie ma bowiem wątpliwości co do tego, że po myśli art. 45 ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (w brzmieniu obowiązującym w dacie zdarzenia), ciężar dowodu w tym zakresie spoczywał właśnie na stronie pozwanej (por. m.in. wyrok Sądu Najwyższego z dnia 18 stycznia 2018 r., V CSK 141/17, LEX nr 2481983). Z obowiązku tego skarżący nie mógł się jednak skutecznie wywiązać ani dowodem z dokumentu w postaci wyciągu z logo systemowego (o czym szerzej w dalszej części pisemnych motywów niniejszego uzasadnienia), ani też dowodem z kolejnej już opinii biegłego sądowego z zakresu informatyki, przy pomocy której dążył do wykazania, że nr IP 83.6.43.157 należał do komputera strony powodowej, z którego przeprowadzono kwestionowane w sprawie transakcje; albowiem – zdaniem Sądu - samo przez się nie oznacza to, że P. D. te przelewy autoryzował.

Prawidłowa była zatem decyzja procesowa Sądu Okręgowego, odmawiająca uwzględnienia takiego wniosku dowodowego strony pozwanej. Dość wskazać, że słuchany na rozprawie przeprowadzonej w dniu 11 grudnia 2018 r. biegły sądowy wyjaśnił, że transakcja wykonana w dniu 22 września 2016 r. z użyciem kodu oznaczonego nr 21 na karcie kodów numerycznych (tzw. „zdrapce"), jak i następująca po niej – oznaczona nr 41, mogły być dokonane z tego samego komputera, na co wskazuje adres IP (protokół rozprawy, k. 322-323). Okoliczność ta nie dowodzi jednak jeszcze – jak chce tego skarżący – że powód autoryzował transakcje, które doprowadziły do wyprowadzenia z jego rachunku bankowego środków objętych żądaniem pozwem.

Tożsame przyczyny legły zresztą u podstaw oddalenia zgłoszonego na etapie postępowania apelacyjnego, wniosku pozwanego o przeprowadzenie dowodu z kolejnej opinii biegłego sądowego tożsamej specjalności, przy pomocy którego skarżący dążył do wykazania omówionej wyżej kwestii.

Jeśli zaś chodzi o sygnalizowane w apelacji niejasności, co do okoliczności, w jakich doszło do utraty kodu autoryzacji transakcji oznaczonego nr 21 (powołując się na dowód z dokumentu w postaci wyciągu z logo systemowego zatytułowanego „Dane dotyczące logowań klienta w przedmiotowych dniach" skarżący wskazuje bowiem, że podczas jednego logowania do systemu bankowości elektronicznej (...) S.A. w dniu 22 września 2016 r., z komputera o tożsamym nr IP, tj. 83.6.43.157 wprowadzono dwie transakcje do systemu internetowego – pierwszą o godzinie 22:42:31, zaś drugą o godzinie 22:45:47 – autoryzowaną kodem nr 41, co jakoby przeczy zeznaniom powoda), to celem wyjaśnienia tej kwestii, korzystając z uprawnienia z art. 232 zd. 2 k.p.c., Sąd Apelacyjny dopuścił z urzędu dowód z przesłuchania w charakterze strony powoda P. D. na okoliczność czynności podejmowanych przez niego w związku z logowaniem w dniu 22 września 2016 r. na własne konto, w serwisie internetowym pozwanego Banku. I jakkolwiek treść tych zeznań potwierdziła częściowo stanowisko pozwanego, ponieważ istotnie 22 września 2016 r., P. D. dwukrotnie posłużył się kartą kodów numerycznych, tzw. „zdrapką"; to jednak wyłącznie druga z tych operacji (tj. dotycząca uiszczenia przez niego opłaty za energię elektryczną) była zgodna z jego wolą, a tym samym przez niego autoryzowana. W tym też celu wykorzystał kod nr 41 z owej karty. Pierwsza zaś, do której powód spożytkował kod oznaczony nr 21, miała mu umożliwić jedynie zalogowanie się do systemu płatności internetowej (protokół rozprawy z dnia 3 października 2019 r., k. 396v); a jak się finalnie okazało została podstępnie sprowokowana przez przestępców w celu wyłudzenia tego kodu i jego dalszego wykorzystana w działalności przestępczej.

Powyższe implikuje stwierdzenie, że całokształt zgromadzonego w sprawie materiału dowodowego pozwolił na wyprowadzenie wniosków przeciwnych, do tych zaprezentowanych w apelacji pozwanego. Ustalenia Sądu I instancji, traktujące przede wszystkim o sposobie wyprowadzenia środków z rachunku bankowego powodów, złożonych w sprawie zawiadomieniach o podejrzeniu popełnienia przestępstwa oraz wniesieniu reklamacji, uzupełnione dodatkowo dopuszczonym w instancji odwoławczej dowodem z przesłuchania powoda w charakterze strony, wykluczyły sugestię apelującego, jakoby powód miał udostępnić innej, postronnej osobie instrument finansowy,

umożliwiający wykonanie serii przelewów, przez które z rachunku bankowego małżonków D. wyprowadzono kwotę zasądzoną przez Sąd Okręgowy.

Słuszność ma również Sąd I instancji, że w sprawie nie wykazano rażącego niedbalstwa powodów w przestrzeganiu obowiązków przewidzianych w art. 42 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych. Otóż błędnie utożsamia apelujący niepoinformowanie go o „nietypowym" komunikacie wyświetlonym podczas próby skorzystania przez powoda z internetowego serwisu płatniczego, z przypisaniem powodom rażącego niedbalstwa. Uwagę zwraca, że powód, przed podaniem kodu oznaczonego nr 21 na karcie kodów numerycznych, upewnił się, że strona internetowa (nieodbiegająca nota bene wyglądem od właściwej strony skarżącego) wyposażona została w stosowne zabezpieczenia w postaci zielonej kłódki i prefiksu witryny „https". W ocenie Sądu Apelacyjnego, powód miał podstawy do uznania, że komunikat ten pochodził od pozwanego Banku; zwłaszcza, że P. D. nie posiadał wówczas wiedzy, że logowanie do serwisu płatniczego nigdy nie wymagało podania kodu z narzędzia autoryzacyjnego. Jak słusznie akcentował Sąd Okręgowy, komunikat o tego rodzaju zagrożeniu pojawił się na stronie internetowej Banku dopiero po zdarzeniu z udziałem małżonków D..

Podobnie, w sprawie nie zostało dowiedzione, aby powodowie nie dochowali należytej staranności we właściwym zabezpieczeniu komputera. Z dokonanych w sprawie ustaleń wynika, że małżonkowie nie informowali nikogo o loginie i haśle do logowania na stronę internetową Banku. Nie udostępniali też nikomu tegoż sprzętu, a w kontaktach internetowych ze skarżącym powodowie (a w zasadzie powód) używali jedynie własnego komputera. Samo zaś przyjęte przez stronę skarżącą założenie o niekorzystaniu przez powodów z aktualnego i legalnego oprogramowania (tak antywirusowego, jak i operacyjnego), czego potwierdzeniem – jak się wydaje – miał być już tylko fakt nieprzedłożenia przez nich certyfikatów lub dowodów zakupu takiego oprogramowania, nie mogło zostać uznane za wystarczające do oddalenia powództwa. Z pola widzenia nie można bowiem tracić, że z przeprowadzonego na etapie postępowania pierwszoinstancyjnego dowodu z opinii biegłego z zakresu informatyki wynika, że w sprawie nie było możliwe rozstrzygnięcie, czy w okresie objętym zdarzeniem z 2016 r. komputer powodów wspierany był przez aktualne i legalne oprogramowanie. Nie było też danych, pozwalających na ustalenie czy we wskazanym okresie komputer ten chroniony był zabezpieczeniami przed nieuprawnionym dostępem osób trzecich. Jak wyjaśnił biegły, zatarcie tych danych z bardzo dużym prawdopodobieństwem spowodowane było reinstalacją systemu operacyjnego, dokonaną przez powoda w dniu 29 września 2016 r., ale także dalszym użytkowaniem komputera i stosunkowo niewielkim dyskiem twardym (80 GB), w który był on wyposażony (pisemna opinia biegłego, k. 268-273).

Sama zatem okoliczność nieprzedłożenia przez powodów przedmiotowej dokumentacji, zważywszy na wykonanie przez powoda, zleconej mu przez wykwalifikowanych pracowników strony pozwanej, reinstalacji oprogramowania komputera, która najprawdopodobniej przyczyniła się do zatarcia danych umożliwiających weryfikację zainstalowanego na tym urządzeniu oprogramowania, nie może być aktualnie poczytywana na niekorzyść małżonków D.. Gdyby bowiem pracownicy pozwanego poinformowali powodów o konieczności zabezpieczenia urządzenia, małżonkowie D. mieliby możliwości współdziałania na tym polu ze skarżącym. Taki postulat nie został jednak do nich skierowany.

Mając to wszystko na uwadze, Sąd Apelacyjny za prawidłową uznał ocenę Sądu Okręgowego, że żądanie powodów zwrotu środków w wysokości dochodzonej pozwem było uzasadnione, a swoją podstawę znalazło w art. 46 ust. 1 ustawy o usługach płatniczych. Powodowie nie naruszyli bowiem obowiązków przewidzianych w art. 42 tej ustawy, a skarżący nie wykazał którejkolwiek z przesłanek wyłączających jego odpowiedzialność.

Dlatego też, działając na podstawie art. 385 k.p.c., Sąd Apelacyjny oddalił apelację strony pozwanej.

O kosztach instancji odwoławczej rozstrzygnął zaś w oparciu o art. 98 § 1 i 3 k.p.c. w zw. z art. 108 § 1 k.p.c., przy uwzględnieniu § 2 pkt 6 w zw. z § 10 ust. 1 pkt 2 Rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności radców prawnych (Dz.U. z 2015 r. poz. 1804 ze zm.).

(...)