Sygn. akt III Ca 716/17

UZASADNIENIE

W pozwie z dnia 20 stycznia 2016 roku powód P. T. wniósł o nakazanie pozwanemu (...) Spółce Akcyjnej w W. przywrócenia obciążonego rachunku płatniczego powoda prowadzonego w pozwanym Banku o nr (...) do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza z dnia 29 stycznia 2014 roku dokonana na kwotę 20 090 zł na nr rachunku bankowego (...) oraz przywrócenia obciążonego rachunku płatniczego powoda prowadzonego w pozwanym Banku o nr (...) do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza z dnia 29 stycznia 2014 roku, dokonana na kwotę 19 856,10 zł, na nr rachunku bankowego (...), oraz o zasądzenie od pozwanego na rzecz powoda kosztów postępowania, w tym kosztów Zastępstwa radcowskiego według norm przepisanych. W uzasadnieniu pozwu powód wskazał, że z pozwanym łączą go dwie umowy – umowa o świadczenie usług bankowych, na podstawie której posiada w pozwanym banku rachunek oszczędnościowo-rozliczeniowy (...) i rachunek bankowy (...), oraz umowa odnawialnego kredytu konsumpcyjnego, na podstawie której pozwany Bank udzielił powodowi kredytu odnawialego na kwotę 50 000 zł w rachunku oszczędnościowo-rozliczeniowym, zwanym łącznie dalej (...) Z (...). Powód podał, że w dniu 29 stycznia 2014 roku niezidentyfikowany sprawca dokonał bez wiedzy i zgody powoda szeregu operacji na wymienionych powyżej rachunkach bankowych – z konta (...) Z (...) przelał łączną kwotę 20 090,00 zł w koszt kredytu odnawialnego na rachunek (...) powoda, a z tego ostatniego dokonał przelewu kwoty 19 856,10 zł na zewnętrzny rachunek bankowy prowadzony przez (...) o numerze (...), wskazując jako odbiorcę nieznaną powodowi osobę fizyczną o nazwisku J. O., a w tytule przelewu (...). Spowodowało to znaczne ograniczenie uprawnienia powoda, wynikającego z umowy kredytu odnawialnego. Powód nigdy nie składał polecenia wykonania wymienionych wyżej operacji bankowych, nie wyrażał na nie zgody i nie wiedział o nich, jak również nigdy w żaden sposób z nich nie skorzystał, nie ustanawiał odbiorcy zdefiniowanego w osobie J. O.. Nigdy też nie udostępnił komukolwiek jakichkolwiek danych umożliwiających lub ułatwiających zalogowanie się do internetowego serwisu transakcyjnego powoda. Powód wskazał, że w dniu zdarzenia zawiadomił pozwany bank o zaistniałym zdarzeniu, składając reklamację zarejestrowaną pod numerem (...) oraz dokonał zawiadomienia o zaistniałej sytuacji na Komendzie Powiatowej Policji w Ż.. Podał, że do dnia wytoczenia powództwa złożona przez niego reklamacja nie została rozpoznana i nie ustalono, w jaki sposób pozwany bank przekazał jego środki osobie do tego nieuprawnionej ani w jaki sposób doszło do nieautoryzowanych przelewów z rachunków bankowych powoda. P. T. podniósł również, że pozwany bank nie zapewnił wymaganego przepisami bezpieczeństwa transakcji dokonywanych na prowadzonych przez niego rachunkach bankowych, nie wdrożył standardowo stosowanych przez inne banki zabezpieczeń przeprowadzanych transakcji i tak skonstruował system bankowości elektronicznej, że przechwycenie przez przestępców jednej wiadomości sms zawierającej kod potwierdzający operację ustanowienia odbiorcy zdefiniowanego, powoduje możliwość przekazania takiemu odbiorcy wszelkich środków ze wszystkich posiadanych przez daną osobę produktów bankowych, bez konieczności dodatkowej weryfikacji takich przelewów. Wskazał, że odpowiedzialność banku wynika z przepisów ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych, która to regulacja przewiduje szeroką odpowiedzialność banku za transakcje nieautoryzowane, przewidując między innymi obowiązek niezwłocznego zwrotu powodowi kwoty nieautoryzowanej transakcji płatniczej, a w przypadku korzystania z rachunku płatniczego – przywrócenia obciążonego rachunku płatniczego powoda do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatniczaą

W odpowiedzi na pozew (...) S.A. wniósł o oddalenie powództwa w całości, zawieszenie postępowania cywilnego z uwagi na toczące się postępowanie karne, którego wynik ma wpływ na rozstrzygnięcie w przedmiotowej sprawie oraz o zasądzenie kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych. Wskazał, że nie ponosi winy za nienależyte wykonanie umowy rachunku bankowego, środki pieniężne zgromadzone na rachunkach klientów banku, w tym na rachunku bankowym powoda były bezpieczne, a w dacie dokonania spornego przelewu nie miało miejsca przełamanie systemów zabezpieczeń pozwanego banku. Podał, że na bieżąco informuje klientów na swoich stronach internetowych o pojawiających się zagrożeniach. Pozwany podniósł, że to powód nie dochował należytej staranności w ochronie swoich newralgicznych danych, w posiadanie których weszły osoby trzecie. Podważany przez powoda przelew miał poprawnie zdefiniowane wszystkie elementy, był wykonany z użyciem

prawidłowych i poprawnych narzędzi autoryzacji, a tak zlecona operacja ze względów technicznych nie mogła podlegać jakiejkolwiek dodatkowej weryfikacji przez system banku. Z ostrożności procesowej pozwany podniósł zarzut przyczynienia się powoda w 100% do powstania szkody poprzez udostępnienie swoich danych, które obowiązek miał chronić, osobom nieuprawnionym, co z kolei umożliwiło wykonanie przedmiotowego przelewu.

W piśmie procesowym z dnia 29 kwietnia 2016 roku powód podniósł, że brak jest podstaw do zawieszenia postępowania i zakwestionował okoliczność, jakoby umyślnie lub wskutek rażącego niedbalstwa naruszył jakiekolwiek postanowienie zawartej z pozwanym umowy. Zakwestionował również wiążący charakter Regulaminu mającego stanowić integralną część tej umowy, o treści załączonej do odpowiedzi na pozew, z uwagi na nieprawidłowości w jego doręczeniu powodowi, a w konsekwencji wskazał, że powód nie miał umownego obowiązku „należytego zabezpieczenia narzędzi i urządzeń, z których korzysta w celu uzyskania dostępu do rachunku, w szczególności poprzez zainstalowanie na urządzeniu legalnego oprogramowania systemowego i antywirusowego". Niezależnie od powyższego podał, że w treści tego Regulaminu nie jest wskazane, czy konsumenci mieli posiadać oprogramowanie antywirusowe płatne czy bezpłatne, a powód korzystał z oprogramowania bezpłatnego. Ponadto, wskazał na wynikającą z art. 8 ustawy o usługach płatniczych nieważność zawartej w Regulaminie regulacji wyłączającej odpowiedzialność Banku z tytułu szkód związanych z postępowaniem Posiadacza Rachunku w sposób sprzeczny z postanowieniami nakładającymi na niego obowiązek opisany powyżej, które wystąpiły z powodu okoliczności niezawinionych przez Bank. Powód podniósł, że bank nie może zwolnić się od obowiązku zapewnienia bezpieczeństwa rachunku niekorzystnymi dla klienta postanowieniami regulaminu, a zgodnie z art. 45 powołanej ustawy ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika, czyli na pozwanym. Powód korzysta zatem z domniemania odpowiedzialności banku za dokonanie nieautoryzowanej transakcji płatniczej, a w świetle ust. 2 powołanego przepisu, nawet dokonanie zarejestrowanego użycia instrumentu płatniczego nie obala tego domniemania. Powód podniósł również zarzut nieprawidłowego wypełnienia przez pozwany bank obowiązków informacyjnych.

W piśmie przygotowawczym z dnia 29 sierpnia 2016 roku pozwany podtrzymał dotychczasowe stanowisko, przedstawione w odpowiedzi na pozew. Podał, że kwestionowany przez powoda regulamin został mu skutecznie doręczony i regulamin załączony przez pozwanego do odpowiedzi na pozew jest prawidłowym regulaminem obowiązującym w dacie zdarzenia. Pozwany wskazał, że powód uchybił swoim obowiązkom wymienionym w art. 42 ust. 2 ustawy, udostępniając instrument płatniczy osobom nieuprawnionym przez niedochowanie należytej ostrożności.

Wyrokiem z dnia 2 stycznia 2017r. Sąd Rejonowy dla Łodzi – Ś. w Ł. nakazał pozwanemu (...) Spółce Akcyjnej w W. przywrócenie obciążonego rachunku płatniczego powoda prowadzonego w pozwanym banku o nr (...) do stanu jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza z dnia 29 stycznia 2014r. dokonana na kwotę 20.090 zł na nr rachunku bankowego (...) oraz przywrócenie obciążonego rachunku płatniczego powoda prowadzoneego w pozwanym Banku o nr (...) do stanu jaki istniałby gdyby nie miała miejsce nieautoryzowana transakcja płatnicza z dnia 29 stycznia 2014r. dokonana na kwotę 19.856,10 zł na nr rachunku bankowego (...).

Nadto Sąd I instancji zasądził od pozwanego (...) Spółki Akcyjnej w W. na rzecz powoda kwotę 5822 zł tytułem zwrrotu kosztów procesu.

Powyższe rozstrzygnięcie Sąd I instancji oparł na nastepujących ustalenaich stanu faktycznego :

W dniu 1 czerwca 2010 roku P. T. zawarł z pozwanym – wówczas M. (obecnie (...) S.A.) – umowę o świadczenie usług bankowych, na podstawie której otwarty został rachunek oszczędnościowo-rozliczeniowy (...) oraz rachunek bankowy (...). W dniu 26 kwietnia 2013 roku strony zawarły umowę odnawialnego kredytu konsumpcyjnego, na podstawie której pozwany Bank udzielił powodowi kredytu odnawialnego na kwotę 50 000 zł w rachunku oszczędnościowo-rozliczeniowym, zwanym łącznie dalej (...) Z (...). Powód mógł dysponować środkami w ramach tego kredytu w formie gotówkowej, bezgotówkowej lub na podstawie polecenia przelewu na dowolny rachunek bankowy. Pozwany bank zapewnił dostęp do obydwu wskazanych powyżej rachunków za pośrednictwem systemu bankowości elektronicznej.

W dniu 11 kwietnia 2013 roku, aktem notarialnym Rep. A nr (...), sporządzonym przez Notariusza w W. T. C., zmieniono między innymi § 1 i § 2 Statutu pozwanego, w wyniku czego, z dniem wpisu tych zmian do Krajowego Rejestru Sądowego zmianie uległa nazwa pozwanego z (...) BANK S.A. (w skład którego wchodziła marka detaliczna M.) na (...) S.A.

W dniu 29 stycznia 2014 roku około godziny 08.30 powód logował się na platformę transakcyjną pozwanego banku i po zalogowaniu (tj. wpisaniu identyfikatora i hasła), na ekranie komputera pojawił się komunikat, że w związku z łączeniem się banków (...) i mBanku, konieczne jest wpisanie do wyświetlonego okienka kodu otrzymanego drogą sms-ową celem zdefiniowania rachunku, w przeciwnym bowiem razie nie będzie możliwe dokonywanie niektórych czynności na stronie banku. Okienko z komunikatem stanowiło nakładkę na rzeczywistą stronę banku i łudząco ją przypominało (ze względu na zastosowane kolory, rozmiar czcionki). Nie było możliwości bezpiecznego pominięcia tego komunikatu, odłożenia wymuszonej przez niego czynności na czas późniejszy, ani zamknięcia go, gdyż po zamknięciu okna przeglądarki, po ponownym zalogowaniu pojawiał się ponownie. Uniemożliwiał on korzystanie z platformy transakcyjnej pozwanego. Aby z niej korzystać, konieczne było wybranie opcji „dalej" czy „wyślij sms", co też powód uczynił. Wówczas na jego telefon komórkowy przyszedł sms, o treści zbieżnej z treścią powyższego komunikatu, zawierający kod sms, który należało wpisać w oknie komunikatu. Powód, pozostając w przekonaniu, że komunikat ten pochodzi od banku, zarówno ze względu na wygląd nakładki z komunikatem, fakt, że otrzymany przez niego sms wyglądał jak inne wysyłane przez bank smsy, jak również wobec powszechnej wówczas informacji o łączeniu się M. i mBanku, wpisał kod z sms-a w okienku komunikatu i mógł dalej korzystać z serwisu transakcyjnego banku.

W wyniku powyższej sytuacji niezidentyfikowany sprawca dokonał bez wiedzy i zgody powoda następujących operacji na posiadanych przez niego w mBanku rachunkach bankowych – z konta (...) Z (...) przelał łączną kwotę 20 090,00 zł w koszt kredytu odnawialnego na rachunek (...), a z tego ostatniego dokonał przelewu kwoty 19 856,10 zł na zewnętrzny rachunek bankowy prowadzony przez (...) o numerze (...), wskazując jako odbiorcę nieznaną powodowi osobę fizyczną o nazwisku J. O., a w tytule przelewu (...).

Przeprowadzona przez pozwany bank analiza wykazała, że dnia 29 stycznia 2014 roku o godzinie 8.30 została złożona dyspozycja zmodyfikowania odbiorcy zdefiniowanego, w wyniku czego zdefiniowany został odbiorca w osobie J. O. o numerze rachunku (...). W trakcie wpisywania kodu otrzymanego w sms-ie powód nie widział, jakie dane definiuje, sms nie zawierał nazwy odbiorcy definiowanego. Stanowiło to najprawdopodobniej wynik działania wirusa, który zainfekował komputer powoda, powodując przełamanie jego zabezpieczeń, niezależnie od używanej przeglądarki internetowej. Wirus ten stworzył opisaną powyżej nakładkę na rzeczywistej stronie banku, wymuszając na powodzie czynność w postaci przejścia dalej i generował skrypt, który wywołał wydanie pozwanemu dyspozycji zmodyfikowania odbiorcy zdefiniowanego i wysłanie sms-a z rzeczywistej bramki bankowej pozwanego. Do wykonania następnie przelewu wewnętrznego w ramach rachunków posiadanych przez powoda w pozwanym banku oraz przelewu zewnętrznego, sprawca musiał posiadać dane w zakresie identyfikatora i hasła, które mógł pozyskać w wyniku wcześniejszego zainfekowania komputera powoda w trakcie standardowego korzystania z jego infrastruktury przez tego ostatniego.

Powód nigdy nie składał polecenia wykonania wymienionych wyżej operacji bankowych, nie wyrażał na nie zgody i nie wiedział o nich, nie miał świadomości, że ustanowił odbiorcę zdefiniowanego w osobie J. O., nie zna osoby o takim nazwisku. Nie podawał nikomu swojego identyfikatora i hasła logowania do banku. W okresie przed zdarzeniem nie miały miejsca żadne włamania do jego mieszkania. P. T. korzysta z legalnego, oryginalnego oprogramowania systemu i legalnego bezpłatnego programu antywirusowego A., który mając dostęp do Internetu, aktualizuje się automatycznie. Powód ma zawsze włączoną zaporę systemu W., tak było również w dniu zdarzenia. Posiadał on wówczas telefon starego typu – N. (...), który nie wykorzystuje żadnego systemu operacyjnego typu Android. W dniu zdarzenia powód zawiadomił o nim pozwany bank za pośrednictwem bankowego systemu telefonicznego mLinia. Reklamacja powoda dotycząca nieautoryzowanych przelewów została zarejestrowana tego samego dnia, pod numerem (...), o czym powód został powiadomiony wiadomością e-mail. Zgodnie z zaleceniami ze strony pozwanego P. T. przeskanował komputer różnymi programami antywirusowymi, ale nic one nie wykryły. Tego samego dnia powód złożył również na Komendzie

Powiatowej Policji w Ż. zawiadomienie o popełnieniu przestępstwa. W wyniku tego zawiadomienia postanowieniem z dnia 3 lutego 2014 roku wszczęto dochodzenie w sprawie o przestępstwo z art. 278 § 1 kk, prowadzone pod sygn. akt KR-529/14 przez KPP w Ż., a nadzorowane przez Prokuraturę Rejonową w Żyrardowie.Klient pozwanego Banku, logując się z komputera do systemu bankowości elektronicznej, musi dokonać autoryzacji za pomocą loginu (identyfikatora) przypisanego do użytkownika, nadawanego przez bank, i statycznego hasła, znanego tylko klientowi. Logując się do systemu, użytkownik wpisuje całe hasło, nie jest ono maskowane. Przelew środków na rachunek innego użytkownika wymaga autoryzacji dokonywanej transakcji, na przykład poprzez kod wysyłany sms-em, który to sposób stosował powód. Przelewy pomiędzy rachunkami własnymi tego samego posiadacza nie wymagają autoryzacji kodem z sms-a. Nie wymagają jej również przelewy dokonywane na rzecz odbiorcy zdefiniowanego, sms-em potwierdza się jedynie samo zdefiniowanie takiego odbiorcy lub jego modyfikację. Do zdefiniowania odbiorcy konieczne jest podanie jego nazwy i numeru rachunku. Poza identyfikatorem i hasłem dostępu do rachunku za pomocą systemu bankowości elektronicznej, pozwany bank nie stosuje dodatkowej weryfikacji w celu zalogowania się do platformy transakcyjnej. Nie stosuje również oprogramowania, które wymusza zmianę hasła dostępu do konta co jakiś czas. W okresie zdarzenia będącego przedmiotem niniejszego postępowania bank nie stosował tokenów do autoryzacji. W dacie zdarzenia nie było w systemie mBanku możliwości wychwytywania złośliwego oprogramowania na komputerach klientów, nie były stosowane alerty.

Przed zdarzeniami z dnia 29 stycznia 2014 roku mBank informował swoich klientów o zagrożeniach związanych z bezpieczeństwem, umieszczając w zakładce (...) przede wszystkim informacje dotyczące nieudostępniania innym osobom loginów i haseł. Nie było tam informacji na temat sytuacji, jaka spotkała powoda w tym dniu. Tego typu zagrożenia opisywane były w zakładce (...) lub „Pomoc/ (...). Pozwany bank nie przekazywał również powodowi takich ostrzeżeń drogą pocztową czy mailową. Ostrzeżenia nie pojawiały się wówczas na stronie banku w taki sposób, jak to ma miejsce obecnie – w sposób wyeksponowany, na stronie głównej, na czerwonym tle.

W okresie zdarzenia będącego przedmiotem niniejszego postępowania pozwany bank stawiał swoim klientom minimalne wymagania w zakresie parametrów komputera w aspekcie możliwości korzystania z serwisu transakcyjnego. W § 41 ust. 1 Regulaminu otwierania i prowadzenia bankowych rachunków dla osób fizycznych w ramach bankowości detalicznej (...) S.A. (mBank – dawny M.), obowiązującego od dnia 25 stycznia 2014 roku i stanowiącego integralną część umowy łączącej strony, zawarta była wzmianka o konieczności posiadania i aktualizowania legalnego programu antywirusowego, bez sugerowanej konkretnej aplikacji i bez wymogu, że ma to być oprogramowanie płatne.

Przy takich ustaleniach stanu faktycznego Sąd I instancji uznał roszczenie za uzasadnione i uwzględnił je w całości.

Apelację od powyższego rozstrzygnięcia wniosła strona pozwana.

Skarżąca zarzuciła rozstrzygnięciu:

I.naruszenie prawa procesowego

a. art. 233 § 1 k.p.c. poprzez dokonanie jednostronnej oceny dowodów w sposób niewszechstronny, a także sprzeczny z zasadami doświadczenia życiowego oraz logicznego rozumowania, polegający w szczególności na:

- pominięcie dowodu z zeznań świadka T. W. w zakresie, w jakim zeznał, że zabezpieczenia banku są zgodne z wymogami polskiego prawa oraz sektora bankowego, a strona logowań banku jest zabezpieczona 256 bitowym kluczem szyfrującym, co świadczy o wysokim poziomie zabezpieczenia stosowanego przez bank,

- błędne ustalenie, że zabezpieczenie transakcji elektronicznych stosowne przez pozwanego przed dniem 29 stycznia 2014r. nie były właściwe oparte na następującym wnioskowaniu - gdyby zabezpieczenia te były właściwe ni doszłoby do dokonania z rachunków powoda transakcji przez nieuprawnione do tego osoby,

b.art. 233 § 1 k.p.c. poprzez błędne ustalenie, oparte wyłącznie na zeznanych powoda, że powód korzystał z legalnego, oryginalnego oprogramowania systemu i legalnego, bezpłatnego oprogramowania antywirusowego, który aktualizował się automatycznie oraz przyjęcie, ze powód miał zawsze włączoną zaporę systemu W., co miało istotne znaczenie dla sprawy, bowiem decydowało o przyjęciu, ze powód wywiązał się z obowiązku należytego zabezpieczenia narzędzi i urządzeń, z których korzystał w celu dostępu do rachunku bankowe,

c.art. 233 § 1 k.p.c. poprzez dokonanie jednostronnej oceny dowodów w sposób niewszechstronny, a także sprzeczny z zasadami doświadczenia życiowego oraz logicznego rozumowania, polegający w szczególności na sprzecznym z treścią zgromadzonego materiału dowodowego przyjęciu, że powód nie wykazał się w sprawie rażącym niedbalstwem w zakresie ochrony dostępu do swojego rachunku, ewentualnie, ze nie przyczynił się do dokonania kwestionowanych w sprawie transakcji,

d.rażące naruszenie przepisów prawa procesowego, które miało istotny wpływ na treść zapadłego w sprawie orzeczenia tj. art. 217 §2 k.p.c. w zw. z art. 227 k.p.c. i art. 278 §1 k.p.c. poprzez oddalenie wniosku dowodowego pozwanego o dopuszczenie i przeprowadzenie dowodu z opinii biegłego do spraw informatyki w zakresie naliczy sposobu użytkowania i zabezpieczenia antywirusowych urządzeń należących do powoda oraz udzielenia wyjaśnień w zakresie sposobu zainfekowania urządzenia powoda zastosowanym w sprawie wirusem zmierzających do udowodnienia faktów mających istotne znaczenie dla rozstrzygnięcia w wyniku uznania, ze w świetle przepisów ustawy o usługach płatniczych rozstrzygniecie sprawy nie wymagała wiadomości specjalnych z zakresu informatyki;

II.naruszenie prawa materialnego:

a. art. 46 ust.1 ustawy o usługach płatniczych poprzez jego błędne zastosowanie i przyjęcie odpowiedzialności pozwanego za kwestionowane w niniejszym postępowaniu transakcje,

b. art. 46 ust.3 ustawy o usługach płatniczych poprzez jego niezastosowanie i uznanie, ze powód nie odpowiada za transakcje nie doprowadziwszy do nich wskutek rażącego niedbalstwa,

c. art. 362 k.pc. poprzez jego niezastosowanie i przyjęcie, że powód nie przyczynił się do powstania szkody w 100%, w sytuacji, gdy z okoliczności sprawy wynika, ze powód przyczynił się do powstania szkody.

W konkluzji skarżąca wniosła o zmianę zaskarżonego wyroku i oddalenie powództwa i zasądzenie kosztów procesu za obie instancję.

W odprowadzi na pozew powód wniósł o oddalenie apelacji i zasądzenie od strony pozwanej na rzecz podkowa kosztów zastępstwa procesowego postepowaniu apelacyjnym.

Sąd Okręgowy zważył, co następuje:

Apelacja nie jest zasadna.

Wbrew zarzutom skarżącego podniesionym w apelacji, Sąd I instancji dokonał prawidłowych ustaleń stanu faktycznego, znajdujących pełne oparcie w zebranym w sprawie materiale dowodowym i trafnie określił konsekwencje prawne z nich wynikające.

Ustalenia stanu faktycznego poczynione przez Sąd I instancj, Sąd Okręgowy przyjmuje za własne bez konieczności ponownego ich przytaczania.

Wbrew zarzutom skarżącego, Sąd I instancji dokonując oceny materiału dowodowego nie naruszył reguły opisanej dyspozycją art. 233 § 1 k.p.c.

Sąd I instancji ustalił stan faktyczny sprawy na podstawie wszystkich przeprowadzonych dowodów, w tym dowodu z zeznań świadka T. W.. Okoliczność posiadania przez pozwany Bank zabezpieczeń zgodnych z wymogami prawa

polskiego oraz sektora bankowego wykazana przez świadka T. W. nie miał żadnego wpływu na wyłączenie, czy ograniczenie odpowiedzialności banku za nieautoryzowane transakcje płatnicze. Ponadto, właściwie Sąd I instancji ocenił, że w sytuacji dopuszczenia przez pozwany bank do przeprowadzenia nieautoryzowanej transakcji płatniczych na rachunkach bankowych powoda prowadzonych przez bank (co stanowi okoliczność bezsporną, potwierdzoną również przez pozwany bank w złożonej apelacji), bank naruszył obowiązki ciążące na nim w zakresie zabezpieczenia instrumentu płatniczego już przez sam fakt przekazania środków osobie nieupoważnionej.

Bezzasadny jest także zarzut skarżącego, że Sąd I instancji błędnie ustalił, iż powód korzystał z legalnego i aktualnego oprogramowania systemowego i antywirusowego w opaci o dowód z zeznań powoda. O. istotne dla sprawy (art. 227 k.p.c. i art. 217 k.p.c.) mogą być udowodnione za pomocą wszelkich dowodów, w tym dowodu z przesłuchania stron i wbrew twierdzeniom strony pozwanej powód nie miał obowiązku wykazywania posiadanego oprogramowania systemowego i antywirusowego za pomocą dowodu z dokumentów. Co więcej, to nie na powodzie spoczywał ciężar udowodnienia faktu korzystania z właściwego oprogramowania systemowego i antywirusowego, ale na pozwanym dążącym do wykazania naruszenia przez powoda obowiązków umownych, w zakresie stosowania odpowiednich środków zabezpieczających. Tymczasem pozwany nie przedstawił żadnego dowodu, który przeczyłby posiadaniu przez powoda legalnego oprogramowania systemowego i antywirusowego, na bieżąco aktualizowanego.

Zasadnie także Sąd I instancji oddalił wnioski powoda i pozwanego o dopuszczenie dowodu z opinii biegłego do spraw informatyki zgłoszone w pozwie i odpowiedzi na pozew. W świetle przepisów ustawy o usługach płatniczych oraz niekwestionowanej przez stronę pozwaną okoliczności faktycznej dopuszczenia przez pozwany bank do przeprowadzenia nieautoryzowanej transakcji płatniczych na rachunkach bankowych powoda prowadzonych przez bank, rozstrzygnięcie sprawy nie wymagało wiadomości specjalnych z zakresu informatyki.

Bezzasadne są także zarzuty naruszenia prawa materialnego.

Zobowiązanie banku względem posiadacza rachunku kształtuje regulacja zawarta w art. 725 k.c. oraz art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997r. – Prawo bankowe, który stanowi, że bank jest zobowiązany do dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Zapewnienie bezpieczeństwa depozytów jest jednym z najistotniejszych obowiązków banku, a sposób jego wykonywania jest najbardziej wymierną podstawą oceny jego wiarygodności. W tym zakresie na banku zawsze spoczywa obowiązek dołożenia wszelkich starań, bowiem profesjonalny charakter jego działalności wymaga stosowania podwyższonego miernika staranności przy wykonywaniu 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 o usługach płatniczych z dnia 19 sierpnia 2011 roku. Przewiduje ona generalną zasadę, że dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika (art. 40 ust. 1). Zgodnie z art. 46 ust. 1 powołanej 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. W razie dokonania wypłaty osobie nieuprawnionej, poszkodowanym tą czynnością jest bowiem bank, a nie osoba, która zdeponowała środki na rachunku.

Zgodnie z art. 45 Ustawy o usługach płatniczych, ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika, spoczywa na dostawcy tego użytkownika, przy czym do zrealizowania tego obowiązku dowodowego nie jest wystarczające wykazanie samego zarejestrowanego użycia instrumentu płatniczego. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których

mowa w art. 42 powołanej ustawy. Powyższa regulacja wprowadza domniemanie odpowiedzialności banku za każdą nieautoryzowaną transakcję i pozwany, chcąc je obalić, musi udowodnić jedną z okoliczności enumeratywnie wymienionych w art. 46 ust. 2 Ustawy o usługach płatniczych.

W niniejszej sprawie bezsporne było, że powód ani nie dokonał, ani nie wyraził zgody na dokonanie transakcji z dnia 29 stycznia 2014 roku w postaci przelewu z rachunku „M. Ja z Kredytem" kwoty 20 090,00 zł w koszt kredytu odnawialnego na rachunek (...), oraz przelewu z tego ostatniego rachunku kwoty 19 856,10 zł na zewnętrzny rachunek bankowy prowadzony przez (...) o numerze (...), na rzecz nieznanej powodowi osoby fizycznej o nazwisku J. O..

Zgodzić należy się z Sądem I instancji, że w świetle materiału dowodowego zebranego w sprawie mBank nie dołożył szczególnej staranności w tym zakresie i nie wywiązał się z tej powinności, skoro przekazał środki zdeponowane przez powoda osobie do tego nieuprawnionej. Sam fakt przekazania tych środków oznacza właśnie brak takiej staranności.

Rację ma także Sąd I instancji i w tym zakresie, że powodowi nie można przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa, a tym bardziej działania umyślnego. Jego komputer miał w dacie zdarzenia zainstalowaną zaporę systemu W. i posiadał zainstalowane, zaktualizowane oprogramowanie antywirusowe, bezpłatne, ale regulamin nie wymagał posiadania oprogramowania płatnego ani nie zalecał żadnej konkretnej aplikacji.Wpisanie przez P. T. do wyświetlonego po zalogowaniu na stronę pozwanego banku okienka kodu z wiadomości sms (którą powód otrzymał na prywatną komórkę, na którą smsy z banku zawsze przechodziły) nie nosi cech rażącego niedbalstwa. Należy zaznaczyć, że nie było możliwości bezpiecznego pominięcia tego komunikatu, zamknięcia go czy odłożenia na czas późniejszy, uniemożliwiał on korzystanie z serwisu transakcyjnego pozwanego. Wyglądał on jak rzeczywista strona banku, a ponadto nawiązywał do przekształcenia pozwanego, która to okoliczność była wówczas powszechnie znana. Z kolei wiadomość sms otrzymana przez powoda pochodziła rzeczywiście od banku i wyglądała jak typowe smsy, które nadawał on przy dokonywaniu transakcji. Powód miał zatem prawo pozostawać w przekonaniu, że komunikat wyświetlający na platformie transakcyjnej pozwanego, nawiązujący do jego przekształcenia, pochodzi właśnie od niego. Jak wynika z materiłu dowodowego zebranego w sprawie, powód nie przekazał nikomu swojego loginu ani hasła do konta bankowego, zostały one przechwycone przez sprawcę wskutek działania na komputerze powoda szkodliwego oprogramowania. Nie naruszył więc obowiązku wskazanego w art. 42 ust. 2 ustawy o usługach płatniczych, zachował wszelkie niezbędne środków służące zapobieżeniu naruszeniu indywidualnych zabezpieczeń instrumentu płatniczego.

Zgodzić należy się z Sądem I instancji , że w rozpoznawanej sprawie brak również podstaw do zastosowania regulacji zawartej w art. 46 ust. 2 ustawy, stanowiącej, że jeżeli nieautoryzowana transakcja jest skutkiem nieuprawnionego użycia instrumentu płatniczego w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2 (nie noszącego cech umyślności ani rażącego niedbalstwa), płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 150 euro. W niniejszej sprawie powód, jako klient banku w ogóle, w żaden sposób nie naruszył tych obowiązków, o czym świadczą powołane powyżej okoliczności. Bezzasadne jest tym samym twierdzenie pozwanego, że powód przyczynił się do powstania szkody.

Nadto, powód spełnił wynikający z art. 42 Ust. 1 pkt 2 i art. 44 ust. 1 ustawy o usługach płatniczych obowiązek niezwłocznego zawiadomienia banku o zaistnieniu nieautoryzowanej transakcji płatniczej.

W tym stanie rzeczy zasadnie Sąd I instancji uznał, że zgodnie z art. 46 ust. 1 Ustawy o usługach płatniczych, pozwany jest zobowiązany niezwłocznie przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miały miejsca nieautoryzowane transakcje płatnicze z rachunków P. T.. Roszczenie to pozostaje aktualne w przypadku, gdy płatnik korzysta z rachunku płatniczego, co miało miejsce w niniejszej sprawie. Zgodnie, bowiem z art. 2 pkt 25 powołanej ustawy rachunkiem takim jest między innymi rachunek bankowy, jeżeli służy on do wykonywania transakcji płatniczych .

Mając na uwadze powyższe okoliczności, Sąd Okręgowy oddalił apelację jako bezzasadną na podstawie art. 385 k.p.c.

O kosztach postępowania apelacyjnego Sąd Okręgowy orzekł na podstawie art. 98 k.p.c. Wysokość wynagrodzenia pełnomocnika powoda został określona na podstawie § 2 pkt 5 w zw. z § 10 ust. 1 pkt 1 rozporządzenia Ministra Sprawiedliwości z dnia 3 października 2016r. w sprawie opłat za czynności radców prawnych (Dz.U. 2016r. poz. 1667).