***Sygnatura akt II C 383/15***

# WYROK
## W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 28 września 2015 roku

***Sąd Rejonowy dla Łodzi – Śródmieścia w Łodzi II Wydział Cywilny***

***w następującym składzie:***

***Przewodnicząca***: SSR Aleksandra Jamróz

***Protokolant:*** sekr. sąd. Aleksandra Natkańska

***po rozpoznaniu w dniu*** 16 września 2015 roku w Łodzi

***na rozprawie***

***sprawy z powództwa*** A. T.

***przeciwko*** Bankowi (...) Spółce Akcyjnej we W.

o zapłatę kwoty 19.700 złotych

1. zasądza na rzecz A. T. od Banku (...) Spółki Akcyjnej we W. kwotę 18.450,81 zł (osiemnaście tysięcy czterysta pięćdziesiąt złotych osiemdziesiąt jeden groszy) z ustawowymi odsetkami od dnia 5 września 2014 roku do dnia zapłaty oraz kwotę (...),88 (trzy tysiące pięćdziesiąt trzy złote osiemdziesiąt osiem groszy) tytułem zwrotu kosztów procesu;

2. oddala powództwo w pozostałej części.

# UZASADNIENIE

Pozwem z 26 marca 2015 r. A. T. wystąpiła przeciwko Bankowi (...) Spółce Akcyjnej we W. o zapłatę kwoty 19.700 zł z odsetkami ustawowymi od dnia 22 maja 2014 r. do dnia zapłaty tytułem odszkodowania za nienależyte wykonanie umowy rachunku bankowego oraz o zasądzenie od pozwanego na jej rzecz zwrotu kosztów procesu. [pozew – k. 2 - 5]

W odpowiedzi na pozew Bank (...) S.A. we W. wniósł o oddalenie powództwa w całości i zasądzenie kosztów postępowania, w tym kosztów zastępstwa procesowego według norm przepisanych. [odpowiedź na pozew – k. 50 - 52]

***Sąd Rejonowy ustalił następujący stan faktyczny:***

Na mocy umowy ramowej rachunków z dnia 4 marca 2003 r. (...) Bank S.A. w W. (obecnie: Bank (...) S.A. we W.) prowadził dla A. T. indywidualny rachunek oszczędnościowo – rozliczeniowy pod nazwą (...) nr (...). W dniu 28 listopada 2006 r. (...) Bank S.A. w W. otworzył na rzecz powódki w ramach umowy rachunku (...) z dnia 4 marca 2003 r. ponadto konto oszczędnościowe nr (...). [okoliczność bezsporna, umowy rachunku – k. 28 – 32, potwierdzenie otwarcia konta oszczędnościowego – k. 33, informacja odpowiadająca odpisowi aktualnemu z Rejestru Przedsiębiorców Krajowego Rejestru Sądowego – k. 55 - 77]

Powódka korzystała w pozwanym Banku z usług bankowości elektronicznej. [okoliczność bezsporna]

Klientom pozwanego, którzy deklarują chęć korzystania z usług bankowości elektronicznej, nie są stawiane żadne wymagania sprzętowe ani dotyczące oprogramowania. Bank sugeruje jedynie, by klient korzystał z programu antywirusowego, aktualnego systemu operacyjnego i przeglądarki. By uzyskać dostęp do usług elektronicznych

banku wystarczy standardowy komputer z popularnym systemem operacyjnym i jedną z pięciu najpopularniejszych przeglądarek. [zeznania świadka B. T. – k. 96]

Aby uzyskać dostęp do konta za pośrednictwem Internetu, klient pozwanego podaje dane identyfikacyjne z tzw. KB karty oraz (...) ustalony przez niego w oddziale Banku. Do autoryzacji transakcji płatniczych konieczne jest natomiast podanie ponadto żądanego hasła (numerów identyfikacyjnych) z listy haseł jednorazowych oraz powtórzenie znaków wyświetlonych na ekranie. Hasła z listy haseł jednorazowych nie są wykorzystywane w pozwanym Banku do identyfikacji klientów na etapie logowania, a jedynie do autoryzacji transakcji. [zeznania świadków: B. T. – k. 95, M. P. – k. 116]

W pozwanym Banku powstają pliki systemowe z listami haseł jednorazowych, tworzone przez biblioteki kryptograficzne. Są one szyfrowane i wysyłane Państwowej Wytwórni Papierów Wartościowych, która drukuje listy i ich identyfikatory, a następnie przekazuje do Banku jako druki tajne w tzw. bezpiecznych kopertach. Pracownicy Banku nie mogą uzyskać dostępu do zawartości koperty. Są one zabezpieczone przez podejrzeniem, a ich naruszenie można stwierdzić „gołym okiem". Dostęp do haseł uzyskuje jedynie klient - posiadacz listy. [zeznania świadka M. P. – k. 116]

Powódka korzystała z narzędzia do autoryzacji transakcji internetowych w postaci haseł jednorazowych, które odbierała w oddziale Banku w formie papierowej. Listę przechowywała najczęściej w domu w szufladzie. [zeznania powódki – k. 119 w związku z wyjaśnieniami informacyjnymi – k. 93]

Pozwany Bank zamieszcza na swoich stronach internetowych ostrzeżenia przed podawaniem przez klientów danych umożliwiających dostęp do ich rachunków bankowych podmiotom innym niż bank, który prowadzi rachunek, przed nietypowymi ekranami żądającymi podania danych służących do autoryzacji dyspozycji (haseł z listy haseł jednorazowych lub tokena), niestandardowymi prośbami o podanie danych dotychczas niewymaganych na stronie logowania, jak hasła jednorazowe wykorzystywane wyłącznie do autoryzacji dyspozycji, złośliwym oprogramowaniem; zamieszcza także informacje wskazujące prawidłowy adres serwisu bankowości elektronicznej („https:/", a nie „http:/") i o konieczności pojawienia się symbolu zamkniętej kłódki w pasku adresowym przeglądarki, odsyła też do komunikatów Komisji Nadzoru Finansowego. Ostrzeżenia są aktualizowane, gdy pojawia się bądź zmienia zagrożenie. Komunikaty wyświetlane są na stronie logowania lub wysyłane bezpośrednio do klienta i prezentowane już po zalogowaniu. Ostrzeżenia tego typu pojawiały się na stronie internetowej Banku także przed 22 maja 2014 r. [wydruki komunikatów – k. 78 – 79, zeznania świadków: B. T. – k. 95 – 97, M. P. – k. 116, M. K. – k. 118 - 119]

Niektóre ostrzeżenia wymagają potwierdzenia, że klient zapoznał się z nimi. Nie jest jednak wykluczone potwierdzenie tej informacji przez cyberprzestępców. [okoliczność bezsporna]

Pozwany Bank posiada specjalne mechanizmy, które sprawdzają zawartość przeglądarki internetowej po stronie klienta pod kątem obecności złośliwego oprogramowania. [zeznania świadka B. T. – k. 95]

Pozwany Bank wymienia informacje na temat przestępczości w sieci z innymi bankami, instytucjami, firmami zewnętrznymi. Bank otrzymał sygnał od firmy zajmującej się bezpieczeństwem w cyberprzestrzeni, że w dniach 22 -23 maja 2014 r. pojawiła się nowa konfiguracja złośliwego oprogramowania. [zeznania świadka B. T. – k. 95-96]

W dniu 22 maja 2014 r. powódka 9-krotnie, a w dniu 23 maja 2014 r. - jednokrotnie, bezskutecznie próbowała logować się, by uzyskać dostęp do swoich rachunków w pozwanym Banku za pośrednictwem Internetu. Na stronie, która wyświetlała się po wpisaniu adresu strony internetowej Banku, powódka podawała login i hasło (dane z KB Karty i (...)), lecz strona zawieszała się, a po pewnym czasie ukazywała się informacja, że nie można uzyskać połączenia z Bankiem. Na żądanie wyświetlone na stronie internetowej powódka przynajmniej dwukrotnie podała też hasło z listy haseł jednorazowych, będącej w jej posiadaniu, jednak w dniach 22 i 23 maja 2014 r. nie uzyskała dostępu do rachunków i nie dokonywała na nich żadnych operacji. [zeznania powódki – k. 119 w związku z wyjaśnieniami

informacyjnymi – k. 93 - 94, zestawienie logowań do rachunku nr (...) w pisemnej informacji pozwanego dla organów ścigania – k. 112 – 114, zeznania świadków: B. T. – k. 95, M. P. – k. 116, M. K. – k. 118]

W dniu 22 maja 2014 r. o godzinie 10:43:50 rachunek oszczędnościowy powódki nr (...) został obciążony na rzecz posiadacza rachunku o numerze (...)(...) (...), posługującego się nazwiskiem V. A., kwotą 9.800 zł.

W dniu 23 maja 2014 r. o godzinie 12:09:00 rachunek oszczędnościowy powódki nr (...) został obciążony na rzecz posiadacza rachunku o numerze (...) 0000 0001 2338 8510, posługującego się nazwiskiem A. T., kwotą 9.900 zł. [historia operacji – k. 34, zeznania świadka M. K. – k. 118, pisemna informacja pozwanego Banku dla organów ścigania – k. 112 - 114]

W dniu 23 maja 2014 r. o godzinie 12:05:41 w serwisie powódki pozwany wyświetlił nowy komunikat bezpieczeństwa dotyczący zagrożenia w sieci. [pismo pozwanego – k. 39 – 40, okoliczność przyznana – k. 97]

Gdy powódka logowała się do konta w dniu 23 maja 2014 r. nie widziała żadnych ostrzeżeń. [zeznania powódki – k. 119 w związku z wyjaśnieniami informacyjnymi – k. 94]

Pieniądze z konta powódki zostały przelane na konta otwarte w pozwanym Banku około dwóch tygodni wcześniej, a następnie – w ciągu kilku godzin od wykonania przelewów - wypłacone w placówkach pozwanego Banku w W. i B.. [zeznania świadków: B. T. – k. 96, M. K. – k. 118, pisemna informacja pozwanego Banku dla organów ścigania – k. 112 – 114, ]

Treści i wygląd strony internetowej, jaka wyświetliła się powódce w dniach 22 – 23 maja 2014 r., jest nie do ustalenia. [zeznania świadka M. K. – k. 119]

W dniu 27 maja 2014 r. powódce udało się zalogować do konta. Stwierdziła wówczas, że z jej rachunku oszczędnościowego, bez jej wiedzy i zgody, wykonano powyższe przelewy na rzecz nieznanych jej beneficjentów. [zeznania powódki – k. 119 w związku z wyjaśnieniami informacyjnymi – k. 93 - 94]

W dniu 27 maja 2014 r. powódka zgłosiła osobiście reklamację w oddziale pozwanego Banku w Ł.. Konta powódki oraz dostęp do usług bankowości elektronicznej zostały zablokowane, a lista haseł jednorazowych unieważniona. Tego samego dnia powódka zgłosiła również sprawę Policji. [zeznania powódki – k. 119 w związku z wyjaśnieniami informacyjnymi – k. 93 – 94, zeznania świadków: B. T. – k. 95 – 96, M. K. – k. 118]

Przed dniem 22 – 23 maja 2014 r. powódka nie otrzymała żadnych wiadomości pocztą elektroniczną dotyczących konta, nie przekazywała innym osobom danych z nim związanych. Na komputerze, z którego powódka próbowała logować się w dniach 22 – 23 maja 2014 r., znajdującym się w jej miejscu pracy, nie korzystała z opcji zapamiętywania hasła dostępu do konta. [zeznania powódki – k. 119 w związku z wyjaśnieniami informacyjnymi – k. 94]

W maju 2014 r. pojawiły się również inne przypadki zniknięcia pieniędzy z kont klientów pozwanego banku wskutek przelewów wykonanych z wykorzystaniem haseł z list haseł jednorazowych, znajdujących się w posiadaniu tych konkretnie klientów. W przeglądarce klienta wyświetlała się strona przypominająca wyglądem stronę internetową Banku, na której pojawiały się prośby o podanie danych identyfikacyjnych do logowania oraz kodu z listy haseł jednorazowych. W maju 2014 r. nie doszło do złamania systemu informatycznego zabezpieczeń Banku, lecz do złamania zabezpieczeń po stronie przeglądarek, z których korzystali klienci.

C., na drugim komputerze przeprowadzał operacje na koncie klienta Banku z wykorzystaniem danych zbieranych przez złośliwe oprogramowanie zainstalowane na komputerze klienta: loginu, hasła, kodu z listy haseł jednorazowych wpisanego przez klienta na podstawionej stronie internetowej. Strona podstawiona posiada jak najwięcej oryginalnych elementów, mogą na niej również pozostać ostrzeżenia, by uwiarygodnić jej wygląd. Do zainstalowania złośliwego oprogramowania na komputerze klienta dochodzi np. wskutek kliknięcia w wyświetlone na stronie internetowej zdjęcie, za pośrednictwem plików przesyłanych pocztą elektroniczną, przez otwarcie zainfekowanego

załącznika np. rzekomej faktury czy zestawienia nierozliczonych płatności. [zeznania świadków: B. T. – k. 95-96, M. P. – k. 116 – 117, M. K. – k. 117 - 118]

Pismem z 5 września 2014 r. pozwany poinformował powódkę o wynikach przeprowadzonych przez Bank analiz dotyczących przyczyn zaistniałej sytuacji, wskazując, że nie można wykluczyć działania złośliwego oprogramowania na komputerze, który był narzędziem do złożenia kwestionowanych przez powódkę dyspozycji, pozostawiając dalsze czynności wyjaśniające organom ścigania. [pismo pozwanego – k. 39 - 40]

Postanowieniem z dnia 28 listopada 2014 r. umorzono dochodzenie w sprawie podejrzenia popełnienia przestępstwa, polegającego na bezprawnym wpłynięciu na automatyczne przetwarzanie i przekazywanie danych informatycznych związanych z prowadzeniem przez Bank (...) S.A. rachunku oszczędnościowego o nr (...) prowadzonego dla A. T. i włamania po przełamaniu elektronicznych zabezpieczeń tego rachunku, z którego następnie dokonano kradzieży pieniędzy w łącznej kwocie 19.700 zł na szkodę (...) S.A. – wobec niewykrycia sprawcy przestępstwa. [postanowienie o umorzeniu dochodzenia – k. 35]

Pismem z 12 grudnia 2014 r. pozwany podtrzymał stanowisko zajęte w piśmie z 5 września 2014 r., odmawiając uznania roszczeń powódki. [pismo pozwanego – k. 41]

Pismem z 29 stycznia 2015 r. powódka wezwała pozwanego do zapłaty kwoty 19.700 zł. Bank odmówił zwrotu środków. [wezwanie do zapłaty z dowodem doręczenia – k. 45 – 47, pismo pozwanego – k. 80, zeznania powódki – k. 119 w związku z wyjaśnieniami informacyjnymi – k. 94]

Zgodnie z „Regulaminem kont dla ludności", obowiązującym w pozwanym Banku i stanowiącym integralną część umowy ramowej rachunków, w przypadku wystąpienia transakcji płatniczej nieautoryzowanej Bank powinien niezwłocznie zwrócić posiadaczowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku, gdy posiadacz korzystał z rachunku płatniczego, przywrócić obciążony rachunek do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. [umowa rachunku – k. 28 – 30, Regulamin kont dla ludności – k. 36-38]

Ustalając powyższy stan faktyczny, Sąd oparł się na dowodach z zeznań powódki, świadków oraz z przedłożonych dokumentów, których treść nie była kwestionowana przez żadną ze stron. Oddaleniu podlegał natomiast wniosek o dopuszczenie dowodu z opinii biegłego z zakresu informatyki ze znajomością problematyki bezpieczeństwa bankowych systemów informatycznych i ich zawartości, przestępczości internetowej, wyszukiwania, odzyskiwania i analizy danych świadczących o aktywności użytkowników komputera oraz bankowości - na okoliczności sprecyzowane w odpowiedzi na pozew (k. 50 – 50 v.). Dowód ten, w ocenie Sądu, nie przyczyniłby się do wyjaśnienia okoliczności istotnych dla rozstrzygnięcia sprawy i był częściowo nieadekwatny dla osiągnięcia założonego celu. Zmierzał bowiem w znacznej mierze, w kształcie wnioskowanym przez pozwanego, do ustalenia faktów, nie zaś ich analizy w świetle wiadomości specjalnych. Pytania, o których postawienie biegłemu wnosił pozwany, miały również po części charakter pytań natury ogólnej, bez bezpośredniego związku z rozpoznawaną sprawą. Ponadto, w świetle przywołanych poniżej przepisów prawa, decydujące dla wyniku procesu było ustalenie przede wszystkim działań powódki i ich ocena z punktu widzenia określonego miernika staranności. Rodzaj stosowanych przez Bank zabezpieczeń informatycznych miał natomiast znaczenie drugoplanowe i został w przekonaniu sądu orzekającego w dostatecznym stopniu wykazany za pomocą zeznań świadków strony pozwanej.

***Sąd Rejonowy zważył, co następuje:***

Powództwo jest usprawiedliwione co do zasady i w przeważającej mierze także co do wysokości.

Roszczenie powódki znajduje oparcie w przepisach ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (t. jedn. Dz. U. z 2014 r., poz. 873 ze zm.). Przywołana ustawa określa między innymi prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych, a także zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych (art. 1 pkt 2 ustawy). Bank krajowy jest dostawcą usług płatniczych w rozumieniu ustawy (art. 4 ust. 1 i ust. 2 pkt 1). Przez usługi płatnicze rozumie się działalność polegającą w szczególności na wykonywaniu transakcji płatniczych,

w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy przez wykonywanie usług polecenia przelewu (art. 3 pkt 2 lit. c).

Płatnikiem w rozumieniu ustawy jest m. in. osoba fizyczna, składająca zlecenie płatnicze, czyli oświadczenie skierowane do dostawcy zawierające polecenie wykonania transakcji płatniczej (art. 2 pkt 22 i pkt 36). Zlecenie płatnicze, zgodnie z art. 2 pkt 10 ustawy, płatnik składa przy użyciu instrumentu płatniczego, którym jest zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego (art. 2 pkt 10).

Strony niniejszego postępowania umówiły się, że zgoda na wykonanie transakcji płatniczych za pośrednictwem usług bankowości elektronicznej świadczonych przez pozwany Bank będzie przez powódkę udzielana – po zalogowaniu się do konta za pomocą danych identyfikacyjnych z KB karty oraz numeru (...) przez podanie kodu z listy haseł jednorazowych i powtórzenie wyświetlonego na stronie zestawu znaków.

Na pozwanym Banku jako dostawcy wydającemu instrument płatniczy ciążył z mocy art. 43 pkt 1 ustawy obowiązek zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, na powódce zaś - jako użytkowniku instrumentu płatniczego – spoczywał obowiązek 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 (art. 42 ust. 1 pkt 1 i 2). W celu spełnienia powyższego obowiązku użytkownik, z chwilą otrzymania instrumentu płatniczego, winien podejmować niezbędne środki zapobiegające naruszeniu indywidualnych zabezpieczeń instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (art. 42 ust. 2).

Jak wynika z poczynionych ustaleń, pozwany Bank wywiązywał się z obowiązku zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, powódka natomiast swoim obowiązkom wymienionym w art. 42 ust. 2 ustawy uchybiła, udostępniając instrument płatniczy osobom nieuprawnionym przez wpisanie przynajmniej dwukrotnie w dniach 22 i 23 maja 2014 r. kodów z listy haseł jednorazowych na podstawionej stronie internetowej. Słowo „udostępnić" oznacza w języku polskim: ułatwić kontakt z czymś lub umożliwić korzystanie z czegoś (za: Słownik języka polskiego, PWN). Tego niewątpliwie, w świetle poczynionych w sprawie ustaleń faktycznych, powódka dopuściła się, choć w sposób niezamierzony i nieświadomy. Ustalenia te zostały poczynione przede wszystkim na podstawie zeznań świadków strony pozwanej – B. T., M. P. i M. K., opartych z kolei na wynikach wewnętrznej procedury wyjaśniającej przeprowadzonej w pozwanym Banku. Jednakże i powódka okoliczności tej nie zaprzeczyła, przyznając, że nie pamięta, czy wpisała kod z karty kodów podczas nieudanych logowań do konta. Udostępnienie przez powódkę za pośrednictwem podstawionej witryny internetowej swoich danych identyfikacyjnych oraz haseł z listy będącej w jej posiadaniu osobom nieuprawnionym o nieustalonej tożsamości umożliwiło tym osobom zalogowanie się do jej konta i wykonanie dwóch przelewów. Czynności te z punktu widzenia systemu informatycznego Banku były przeprowadzone poprawnie, przy wykorzystaniu właściwych narzędzi autoryzacyjnych. Mimo tego, kwestionowanych transakcji płatniczych wykonanych z konta powódki w dniach 22 i 23 maja 2014 r. nie można uznać za transakcje autoryzowane.

Zgodnie z art. 40 ust. 1 analizowanej ustawy, transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji w sposób przewidziany w umowie między płatnikiem a jego dostawcą. W świetle poczynionych w sprawie ustaleń powódka takiej zgody nie wyraziła. Świadczy o tym również fakt, że niezwłocznie powiadomiła pozwanego oraz Policję, stosownie do obowiązków wynikających z art. 44 ust. 1 przywoływanej ustawy, celem wyjaśnienia przyczyn zniknięcia z konta niemal całych posiadanych przez nią oszczędności.

W myśl art. 45 ustawy o usługach płatniczych, ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Wykazanie przez

dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana.

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.

W ocenie Sądu oczywistym jest, że w okolicznościach niniejszej sprawy nie można powódce przypisać zgody ani woli podjęcia czynności zmierzających do przeprowadzenia kwestionowanych transakcji płatniczych przy użyciu posiadanych przez nią instrumentów płatniczych, a które to okoliczności świadczyłyby o autoryzowaniu przez nią transakcji. Nie można jej również przypisać umyślnego doprowadzenia do nieautoryzowanych transakcji płatniczych, a to choćby z tej przyczyny, że o ich dokonaniu powódka dowiedziała się dopiero w dniu 27 maja 2014 r. Zostały one zatem przeprowadzone bez jej wiedzy. Nie można jej również przypisać rażącego niedbalstwa w naruszeniu obowiązków, wynikających z art. 42 ustawy. Wprawdzie powódka, jak wskazano powyżej, udostępniła osobom nieuprawnionym dane z listy haseł jednorazowych, czego nie powinna czynić, jednak nie nastąpiło to w okolicznościach świadczących o rażącym niedbalstwie z jej strony.

Jak wynika ze zgromadzonego w sprawie materiału dowodowego, do zainfekowania komputera użytkownika usług bankowości elektronicznej może dojść w podstępny, lecz prosty sposób, np. przez kliknięcie przez użytkownika w zdjęcie na ekranie czy otwarcie załącznika do wiadomości nadesłanej pocztą elektroniczną, informującej np. o nierozliczonych płatnościach czy zawierającej rzekome faktury. Powódka w okresie poprzedzającym kwestionowane transakcje nie otrzymała żadnej wiadomości dotyczącej bezpośrednio jej kont w pozwanym Banku ani nie przekazywała pocztą elektroniczną informacji ich dotyczących. Powódka nie udostępniła nikomu swojej listy haseł jednorazowych w formie papierowej ani jej nie zagubiła. W dniach 22 i 23 maja 2014 r. korzystała z komputera w swoim miejscu pracy, jak twierdzi, a czemu pozwany nie zaprzeczył - z legalnym oprogramowaniem i zabezpieczonego programem antywirusowym, choć Bank nie stawiał swoim klientom niemal żadnych wymagań dotyczących sprzętu i oprogramowania. W komputerze użytym przez powódkę login i hasło dostępu do konta nie były zapamiętane ani podpowiadane. Po wprowadzeniu do komputera adresu strony internetowej Banku wyświetliła się witryna imitująca stronę Banku, o treści i wyglądzie dziś już niemożliwym do odtworzenia, na której żądano podania przez powódkę zwyczajowych danych do logowania (identyfikatora z KB Karty i (...)u) oraz dodatkowego uwierzytelnienia swojej tożsamości przez wpisanie kodu z listy haseł jednorazowych. Żądanie to, wobec trudności z uzyskaniem połączenia, mogło przedstawiać się wiarygodnie. Jak zeznawali świadkowie, na stronach podstawionych hackerzy pozostawiają jak najwięcej elementów oryginalnych, niekiedy również ostrzeżenia przed zagrożeniami w sieci, aby uwierzytelnić ich wygląd. Wprawdzie świadek M. K. zeznała, że strony takie cechuje często nieporadność językowa i stylistyczna, brak jednak dowodów, by z taką właśnie niepoprawnie zredagowaną stroną zetknęła się powódka. Bezspornym jest, że w maju 2014 r. nie tylko powódka padła ofiarą ataku cyberprzestępców, lecz także kilkunastu innych klientów pozwanego Banku. Przemawia to za tym, że strona nie przedstawiała się jako oczywiście fałszywa. Jak wynika z ustaleń, komunikat dotyczący tego zagrożenia, z którym zetknęła się powódka, został skierowany bezpośrednio do niej i do klientów Banku już po zrealizowaniu przez Bank obu spornych przelewów, tj. w dniu 23 maja 2014 r. po godz. 12.00. Wprawdzie na stronach Banku zamieszczano ostrzeżenia przed podawaniem dodatkowych danych identyfikacyjnych także przed 22 maja 2014 r., jednak to właśnie na stronie Banku (a w rzeczywistości na stronie ją imitującej), a nie w innym miejscu i okolicznościach, zażądano od powódki podania konkretnego hasła z wydanej jej przez Bank listy haseł jednorazowych. W ocenie Sądu, powyższe okoliczności, nie pozwalają na przypisanie powódce rażącego niedbalstwa w związku z wpisaniem na stronie internetowej imitującej stronę Banku kodów służących co do zasady do autoryzacji transakcji, a nie do weryfikacji tożsamości.

Zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych oraz postanowieniami regulaminu stanowiącego integralną część łączącej strony umowy rachunku bankowego, 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.

Jeżeli jednak płatnik doprowadził do nieautoryzowanej transakcji umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42, odpowiada on za nieautoryzowane transakcje płatnicze w pełnej wysokości (art. 46 ust. 3). Jak zaznaczono powyżej, przepis ten nie może mieć zastosowania w niniejszej sprawie wobec braku podstaw do przypisania powódce umyślności czy rażącego niedbalstwa.

Jeżeli nieautoryzowana transakcja jest skutkiem nieuprawnionego użycia instrumentu płatniczego w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2, płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji. Ponieważ powódka, jak zaznaczono powyżej, choć w sposób niezamierzony i nieświadomy, dopuściła się, obiektywnie rzecz ujmując, naruszenia jednego ze swoich obowiązków ciążących na niej z mocy art. 42 ust. 2 ustawy o usługach płatniczych, winna ponieść odpowiedzialność za nieautoryzowane przelewy z jej konta do wysokości wyżej wskazanej. Abstrahując od oceny aksjologicznej powyższej regulacji, trzeba wskazać, że ustawodawca zadecydował o takim właśnie rozkładzie ryzyka nieautoryzowanych transakcji między płatnikiem i dostawcą usługi płatniczej w razie naruszenia przez płatnika jednego z jego obowiązków, choćby w sposób niezawiniony (nawet w razie posłużenia się przez osobę nieuprawnioną skradzionym płatnikowi instrumentem płatniczym – art. 46 ust. 2 pkt 1).

Mając na uwadze powyższe regulacje i rozważania, Sąd zasądził na rzecz powódki kwotę 18.450,81 zł, pomniejszając żądane przez powódkę 19.700 zł zgodnie z dyspozycją art. 46 ust. 2 ustawy w następujący sposób:

- 9.800 zł przelane z konta w dniu 22 maja 2014 r. o 626,33 zł, odpowiadające równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego 4, (...), ogłaszanego przez NBP i obowiązującego w dniu wykonania tej transakcji (Tabela nr (...) z dnia 22 maja 2014 r.),

- 9.700 zł przelane z konta w dniu 23 maja 2014 r. o 622,86 zł, odpowiadające równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego 4, (...), ogłaszanego przez NBP i obowiązującego w dniu wykonania tej transakcji (Tabela nr (...) z dnia 23 maja 2014 r.). W zakresie kwoty 1249,19 zł (626,33 zł + 622,86 zł) żądanej tytułem należności głównej powództwo podlegało oddaleniu.

Ponieważ pozwany dopuścił się opóźnienia w zwrocie zasądzonej wyrokiem kwoty, powódce należały się odsetki w wysokości ustawowej zgodnie z art. 481 § 1 i 2 k.c. W myśl cytowanego już art. 46 ust. 1 ustawy, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej „niezwłocznie". Pojęcie to ma charakter niedookreślony, nie wyznacza żadnego sztywno zakreślonego horyzontu czasowego i winno zostać wypełnione treścią w odniesieniu do konkretnych okoliczności sprawy. W ocenie sądu, Bank winien zwrócić płatnikowi kwotę należną mu w świetle art. 46 ustawy po upływie czasu niezbędnego do ustalenia, czy w danych okolicznościach wystąpił przypadek, o którym mowa w tym przepisie, tj. czy wystąpiła transakcja płatnicza nieautoryzowana. Bank winien mieć zatem możliwość podjęcia czynności wyjaśniających. Mając powyższe na względzie, sąd zasądził na rzecz powódki odsetki ustawowe na podstawie art. 481 § 1 i 2 k.c. w zw. z art. 46 ust. 1 ustawy o usługach płatniczych od dnia 5 września 2014 r. (do dnia zapłaty). W tej dacie Bank wystosował do powódki odpowiedź na reklamację, informując o poczynionych we własnym zakresie ustaleniach. Wówczas pozwany niewątpliwie posiadał już wiedzę o okolicznościach niezbędnych dla ustalenia własnej odpowiedzialności. Odmawiając powódce zwrotu środków pieniężnych, popadł z tą chwilą w opóźnienie. Żądanie odsetek w dalej idącym zakresie podlegało oddaleniu.

O kosztach orzeczono w oparciu o art. 100 k.p.c. zgodnie z zasadą stosunkowego ich rozdzielenia. Powódka wygrała proces w 94%. Na poniesione przez nią koszty złożyły się: 985 zł opłaty sądowej od pozwu, 2.400 zł wynagrodzenia pełnomocnika /§ 6 pkt 5 rozporządzenia Ministra Sprawiedliwości z 28 września 2002 r. w sprawie opłat za czynności radców prawnych oraz ponoszenia przez Skarb Państwa kosztów pomocy prawnej udzielonej przez radcę prawnego

ustanowionego z urzędu (t. jedn. Dz. U. z 2013 r., poz. 490)/ oraz 17 zł wydatku na poczet opłaty skarbowej od pełnomocnictwa. Pozwany poniósł koszty równe wynagrodzeniu pełnomocnika (2.400 zł). Łącznie strony poniosły koszty w kwocie 5.453,88 zł, z czego powódkę winno obciążać jedynie 348,12 zł (6%). Do zwrotu na jej rzecz od pozwanego pozostała zatem kwota 3053,88 zł, odpowiadająca różnicy między kosztami, które powódka winna ponieść a kosztami przez nią poniesionymi (3.402 zł – 348,12 zł).