Sygn. akt I C 566/17

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 12 maja 2018 roku

Sąd Okręgowy w Warszawie I Wydział Cywilny

w składzie następującym:

Przewodniczący:SSO Ewa Ligoń-Krawczyk

Protokolant:sekr. sądowy Katarzyna Maciaszczyk

po rozpoznaniu w dniu 12 maja 2018 roku w Warszawie

na rozprawie

sprawy z powództwa T. L.

przeciwko (...) S.A. z siedzibą w W.

o zapłatę

I. zasądza od (...) S.A. z siedzibą w W. na rzecz T. L. kwotę 106.929,77 (sto sześć tysięcy dziewięćset dwadzieścia dziewięć i 77/100) złotych wraz z ustawowymi odsetkami za opóźnienie od dnia 21 sierpnia 2016 roku do dnia zapłaty,

II. oddala powództwo w pozostałym zakresie,

III. zasądza od (...) S.A. z siedzibą w W. na rzecz T. L. kwotę 10.633,05 (dziesięć tysięcy sześćset trzydzieści trzy i 5/100) złotych tytułem zwrotu kosztów procesu.

Sygn. akt I C 566/17

UZASADNIENIE

Pozwem z dnia 8 czerwca 2017 roku powód T. L. wniósł przeciwko (...) S.A. z siedzibą w W. o zapłatę kwoty 107.549,38 złotych wraz z ustawowymi odsetkami za opóźnienie od dnia 21 sierpnia 2016 roku do dnia zapłaty oraz zasądzenie kosztów procesu według norm przepisanych w tym kosztów zastępstwa procesowego.

W uzasadnieniu pozwu pełnomocnik powoda wskazał, iż dochodzi zapłaty z tytułu zwrotu nieautoryzowanych przez powoda transakcji płatniczych, dokonanych z rachunku powoda prowadzonego przez pozwany bank. Powód powołał się na przepisy ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych. (pozew k. 2-43 akt sprawy)

W odpowiedzi na pozew, pełnomocnik pozwanego banku wniósł o oddalenie powództwa oraz zasądzenie kosztów procesu. Pozwany podniósł, iż powód swoim działaniem umożliwił przestępcom kradzież środków pieniężnych ze swojego rachunku bankowego. Powód zatwierdził kodem sms przystąpienie do ubezpieczenia, co skutkowało dodaniem odbiorcy definiowanego i ujawnieniem przez powoda nieznanym osobom loginu i hasła, które to dane winny być przez powoda szczególnie chronione. Pozwany podniósł jednocześnie zarzut przyczynienia się powoda w stu procentach do powstania szkody poprzez niezachowanie należytej staranności w ochronie swoich danych, co doprowadziło do ich udostępnienia osobom nieuprawionym, co z kolei umożliwiło wykonanie przedmiotowych przelewów. Bank nie można obarczać odpowiedzialnością za brak należytej staranności, albowiem to klient banku

bezrefleksyjnie udostępnił swoje dane, które winny być przez niego szczególnie chronione. (odpowiedź na pozew k. 49-76 akt sprawy)

W toku dalszego postępowania strony podtrzymały dotychczasowe stanowiska w sprawie.

Sąd Okręgowy ustalił następujący stan faktyczny:

W dniu 8 listopada 2011 roku powód zawarł z (...) Bankiem S.A. z siedzibą w W., które następcą prawnym jest (...) S.A. z siedzibą w W. umowę o prowadzenie bankowego rachunku oszczędnościowo-rozliczeniowego. (okoliczność bezsporna, umowa k. 15-17v akt sprawy) W ramach tej umowy powód korzystał z usług bankowości elektronicznej. Do systemu transakcyjnego powód logował się z dwóch komputerów o numerach: (...) i (...). (okoliczność bezsporna)

Zgodnie z § 24 Regulaminu otwierania i prowadzenia bankowych rachunków dla osób fizycznych w ramach bankowości detalicznej (...) S.A. obowiązującego od 8 kwietnia 2015 roku, zabezpieczeniu bezpieczeństwa dyspozycji składanych do rachunku służy Identyfikacja Użytkownika Rachunku i potwierdzenie złożenia dyspozycji przez Użytkownika Rachunku. Identyfikator przeznaczony jest wyłącznie dla Użytkownika Rachunku, nie może być ujawniany w żadnej formie, treści ani postaci osobom trzecim, w tym członkom rodziny, jest nadawany z zachowaniem procedur zapewniających zachowanie jego poufności z wykorzystaniem programów komputerowych. Hasło, hasła jednorazowe oraz numer PIN do aplikacji mobilnej: przeznaczone są wyłącznie do użytkownika rachunku, nie mogą być ujawniane w żadnej formie, treści ani postaci osobom trzecim, w tym członkom rodziny, nie są znane organom ani pracownikom banku, jak również innym podmiotom działającym na zlecenie banku, są nadawane z zachowaniem procedur zapewniających zachowanie ich poufności z wykorzystaniem programów komputerowych a uzyskanie informacji o jednym z nich nie pozwala na równoczesne uzyskanie informacji o innym. Użytkownik rachunku zobowiązany jest do podjęcia niezbędnych środków służących zapobieżeniu naruszeniu indywidualnych zabezpieczeń identyfikatora, hasła, haseł jednorazowych oraz numeru PIN do aplikacji mobilnej w szczególności zaś zobowiązany jest do przechowywania z zachowaniem należytej staranności, w tym do nie stosowania aplikacji i innych mechanizmów umożliwiających zapamiętywanie identyfikatora, hasła, haseł jednorazowych oraz numeru PIN do aplikacji mobilnej na komputerze, telefonie lub innym urządzeniu mobilnym za pośrednictwem którego użytkownik rachunku uzyskuje dostęp do rachunku. (regulamin k. 70 akt sprawy)

Zgodnie z par. 27 ww. regulaminu, użytkownik jest zobowiązany do należytego zabezpieczenia narzędzi i urządzeń z których korzysta w celu uzyskania dostępu do rachunku w szczególności poprzez: nie omijanie fabrycznych zabezpieczeń urządzeń telekomunikacyjnych, zainstalowanie na urządzeniu legalnego oprogramowania systemowego oraz antywirusowego, pobranie aplikacji mobilnej w sposób wskazany przez Bank za pośrednictwem strony internetowej banku oraz BOK, dokonywanie aktualizacji zainstalowanego na urządzeniu legalnego oprogramowania systemowego oraz antywirusowego. (regulamin k. 70v akt sprawy)

W dniu 3 czerwca 2015 roku powód zamierzał zlecić wykonanie przelewu poprzez internet. Korzystał z komputera służbowego będącego własnością Instytutu (...). Na komputerze zainstalowany był system W. (...) (...) pozyskany z legalnego źródła w ramach programu (...) oferowany przez M.. Dostawcą internetu była (...) ((...)) z siedzibą w W.. Przed włączeniem przeglądarki internetowej sprawdził, czy jest aktywny program antywirusowy. Zainstalowany na komputerze program A. był aktywny. Przed zalogowaniem się do serwisu banku i podaniem loginu i hasła sprawdził czy połączenie jest szyfrowane. (zeznania świadka A. L. k. 112, nagranie 00:31:20-00:35:04, oświadczenie k. 86-88 akt sprawy) Po prawidłowym zalogowaniu się przez powoda z użyciem danych uwierzytelniających, identyfikatora i hasła, o godz. 14:16. Wyświetlił się komunikat z którego wynikało, że z uwagi na wzrastającą ilość nieuczciwych transakcji z rachunków klientów wszystkie transakcje dokonywane za pośrednictwem serwisu internetowego podlegają dodatkowemu ubezpieczeniu. Komunikat był identyczny jak komunikaty generowane przez bank. Powód dwukrotnie próbował ominąć komunikat. Jednocześnie po minucie od zalogowania została zainicjowana operacja „create contact", próba utworzenia użytkownika zaufanego. Automatycznie przez system bankowy został wygenerowany sms z jednorazowym kodem i szczegółami i typem operacji. Po tym nastąpiło wylogowanie z systemu transakcyjnego i zalogowanie ponowne prawidłowe zalogowanie. Ponownie została zainicjowana operacja „create

contact” i wygenerowanie smsa. Transakcja została przerwana. Po raz trzeci powód zalogował się do systemu, została zainicjowana operacja „cerate contact” i system banku ponownie wygenerował smsa, z nowym kodem do zatwierdzenia operacji o treści: „Operacja nr 3 z dn. 03-06-2015 Definicja odbiorcy i przelewu zdef. Z rach.:... (...) na rach.(...)h. (...) Tym razem powód autoryzował operację poprzez przepisanie kodu do serwisu transakcyjnego. Na skutek tego o godz. 14.20 został utworzony nowy zdefiniowany zaufany użytkownik na koncie powoda. Po utworzeniu nowego użytkownika zdefiniowanego i zaufanego, co wiązało się z tym, że przy wykonaniu kolejnych operacji z tym użytkownikiem nie będą wymagane dalsze poświadczenia. Po kolejnej minucie powód wykonał przelew zapłaty za mieszkanie, po jego wykonaniu wylogował się. (okoliczności bezsporne, zeznania świadka M. P. k. 112-113v, nagranie 00:35:46-01:06:48)

W dniu 4 czerwca 2015 roku z urządzenia o nr IP (...) nastąpiło dwukrotne zalogowanie do serwisu transakcyjnego mBanku z wykorzystaniem identyfikatora powoda i hasła. Podczas tych sesji z konta powoda zostały wykonane 4 przelewy w wysokości kolejno: 24.950 złotych, 27.340 złotych, 27.440 złotych i 28.10 złotych. Przelewy te zostały dokonane na rachunek bankowy, którego właścicielem był J. W.. Operacje te nie wymagały potwierdzenia albowiem były dokonywane do odbiorcy zaufanego. Zostały wykonane przez hakerów używających dane identyfikacyjne i hasło powoda pozyskane przy wykorzystaniu szpiegowskiego oprogramowania zainstalowanego na komputerze z którego korzystał powód, za pośrednictwem podstawionej witryny internetowej. (okoliczność bezsporna, potwierdzenie wykonania operacji k. 20-23, zeznania świadka M. P. k. 112-113v, nagranie 00:35:46-01:06:48 akt sprawy)

Fakt ten powód ustalił w dniu 9 czerwca 2015 roku, po zalogowaniu się na konto i w tym samym dniu niezwłocznie udał się do siedziby banku, gdzie złożył reklamacje czterech nieautoryzowanych przelewów. Tego samego dnia złożył zawiadomienie o popełnieniu przestępstwa na Komendzie Rejonowej Policji nr (...) w W.. Wszczęto postępowanie karne nadzorowane przez Prokuraturę Rejonową P. w W., prowadzone pod sygn. 6 Ds. 961/15. Postępowanie to, wraz z innymi sprawami klientów banków na szkodę których dokonano nieautoryzowanych przelewów, od czerwca 2016 roku prowadzone jest przez Prokuraturę Krajową Wydział Zamiejscowy Departamentu ds. Przestępczości Zorganizowanej i Korupcji w L. po sygnaturą PK II WZ Ds. 7.2016. (okoliczność bezsporna, akta sprawy karnej załączone do akt sprawy PK II WZ Ds. 7.2016 Prokuratury Krajowej, reklamacja k. 24 akt sprawy)

Pozwany bank nie uwzględnił reklamacji powoda złożonej w dniu 9 czerwca 2015 roku w oddziale pozwanego, ani sformułowanej w dalszych pismach procesowych. (okoliczność bezsporna k. 24-32 akt sprawy)

Bank posiada prawidłowe zabezpieczenia systemu, który jednak uniemożliwia kontrolę transakcji jeśli są one nieautoryzowane i związane z zainfekowaniem systemu z którego korzysta klient. Z punktu widzenia banku identyfikacja klienta jak i autoryzacja transakcji przebiegała zgodnie z procedurą. Logowanie do portalu bankowego nastąpiło przy użyciu prawidłowego loginu i hasła z wykorzystaniem szyfrowanego połączenia. Kod autoryzacji został wysłany wiadomością sms-ową na wskazany numer telefonu. (zeznania świadka M. P. k. 112-113v, nagranie 00:35:46-01:06:48)

W toku postępowania karnego powód odzyskał kwotę 330,62 złotych. (okoliczność bezsporna)

Na swoich stronach internetowych, w zakładce aktualności, pozwany informował o zasadach bezpiecznego korzystania z bankowości elektronicznej oraz dwukrotnie w lutym 2015 roku i 26 maja 2015 roku o istniejącym zagrożeniu w ramach o kampanii „phishing”, której celem było podstawienie klientom banku komunikatów o obowiązkowym ubezpieczeniu transakcji w celu uzyskania od nich danych wrażliwych od klientów banków. Wspólnym mianownikiem tej kampanii było rozsyłanie po przypadkowych użytkownikach wiadomości e-mail podszywającej się pod firmę kurierską, była to na przykład informacja o nieodebranej przesyłce w załączniku do wiadomości kryło się złośliwe oprogramowanie, które infekowało w tle użytkownika i wpływało na późniejsze działanie przeglądarki. W momencie wejścia klienta na stronę któregoś z banków, które obejmowała kampania, prezentowana była strona z łatką to jest w miejscu w którym podaje się zwyczajowo dane uwierzytelniające jest wklejony obcy fragment strony, który najpierw wyłudza dane do logowania, a następnie po zalogowaniu do systemu transakcyjnego wyświetla kolejną łatkę z komunikatem, w szacie graficznej danego banku, który ma przekonać klienta by podał w następnych kroku kod z

smsa, czy inne dane to jest wyłudzić newralgiczne dane - w tym wypadku była prośba o podanie kodu sms. (wydruki komputerowe k. 72-74, zeznania świadka M. P. k. 112-113v, nagranie 00:35:46-01:06:48 akt sprawy) Informacje te nie były łatwo dostępne dla klientów, w formie czytelnego ostrzeżenia. (zeznania świadka A. L. k. 112, nagranie 00:31:20-00:35:04, oświadczenie k. 86-88 akt sprawy) Znajdowały się w zakładce aktualności, którą trzeba było rozwinąć, by do niej dotrzeć. (zeznania świadka M. P. k. 112-113v, nagranie 00:35:46-01:06:48 akt sprawy)

Powyższy stan faktyczny sąd ustalił na podstawie okoliczności niespornych jak również na podstawie dokumentów prywatnych i urzędowych których wiarygodności i prawdziwości strony nie kwestionowały, tym samym brak było podstaw do ich kwestionowania przez sąd, jak również na podstawie zeznań ze świadków zawnioskowanych przez strony. Zeznania świadków sąd uznał za wiarygodne, albowiem były jasne i konsekwentne, nad to znajdowały potwierdzenie pozostałym materiale dowodowym zebranym w sprawie.

Sąd oddalił wniosek strony pozwanej o dopuszczenie dowodu z opinii biegłego z zakresu informatyki, posiadającego wiedzę z zakresu bankowości elektronicznej i bezpieczeństwa systemów informatycznych w bankach na okoliczność ustalenia, czy zabezpieczenia transakcji elektronicznych stosowane przez pozwanego w czerwcu 2015 roku odnoszące się do rachunku bankowego powoda były właściwe; czy pomimo stosowania przez bank nowoczesnych zabezpieczeń systemu informatycznego istnieje w praktyce możliwość zainstalowania oprogramowania szpiegowskiego i ataku hakerskiego na komputer powoda, której bank nie może zapobiec; sposobu, w jaki osoba, która zrealizowała kwestionowane przez powoda przelewy na jego szkodę miała dostęp do danych niezbędnych do wykonania na tym rachunku operacji, w tym identyfikatora i hasła do rachunku pozwalających na wykonanie kwestionowanych przez powoda przelewów z jego rachunku. Zdaniem sądu okoliczności te nie miały znaczenia dla rozstrzygnięcia przedmiotowej sprawy, z uwagi na odpowiedzialność pozwanego niezależnie od stosowanych przez niego środków celem zabezpieczenia systemu transakcji internetowych.

Sąd Okręgowy zważył co następuje:

Powództwo w przeważającej części zasługiwało na uwzględnienie.

Strony łączyła umowa prowadzenie bankowego rachunku oszczędnościowo-rozliczeniowego. Strony ustaliły, że zgoda na wykonanie transakcji płatniczych za pośrednictwem usług bankowości elektronicznej świadczonych przez pozwany bank będzie przez powoda udzielana za pośrednictwem strony internetowej banku po zalogowaniu się do konta przy użyciu danych identyfikacyjnych, loginu i hasła. Na pozwanym jako dostawcy wydającemu instrument płatniczy ciążył na mocy art. 43 pkt 1 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych, obowiązek zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, na powodzie natomiast – jako użytkownikowi instrumentu płatniczego- spoczywał obowiązek korzystania z instrumentu płatniczego zgodnie z umową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego dostępu do tego instrumentu. (art. 42 ust. 1 pkt 1 i 2 ww. ustawy) Użytkownik, z chwilą otrzymania instrumentu płatniczego, winien podejmować niezbędne środki, zapobiegające naruszeniu indywidulanych zabezpieczeń instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nie udostępniania go osobom nieuprawnionym. (art. 42 ust. 2 ww. ustawy)

Jak ustalono w toku postępowania dowodowego, bank wywiązał się obowiązku zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Powód natomiast uchybił obowiązkom o których mowa w art. 42 ust. 2 ustawy, umożliwiając osobom nieuprawnionym w sposób niezamierzony i nieświadomie dostęp do jego konta poprzez wpisanie zdefiniowanego zaufanego odbiorcy.

Z okoliczności sprawy wynika, iż powód nie autoryzował przedmiotowych transakcji, zostały one dokonane przez osoby trzecie wbrew wiedzy i woli powoda. Udostępnienie przez powoda za pośrednictwem podstawionej witryny internetowej swoich danych identyfikacyjnych oraz hasła osobom nieuprawnionym umożliwiło tym osobom zalogowanie się do konta powoda i dokonanie przestępstwa polegającego na przelaniu znajdujących się na rachunku

powoda środków pieniężnych na inne konto bez jego wiedzy i woli. Czynności te z punktu widzenia systemu informatycznego banku zostały wykonane poprawnie przy wykorzystaniu właściwych narzędzi autoryzacyjnych. Mimo tego transakcji tych w ocenie sądu nie można uznać za transakcje autoryzowane w rozumieniu art. 40 ust. 1 ww. ustawy. Transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na jej wykonanie w sposób przewidziany umową. Powód nie wyraził zgody na wykonanie tych transakcji, o czym świadczy jego natychmiastowa reakcja po stwierdzeniu kradzieży, osobiste powiadomienie pozwanego w oddziale banku oraz zawiadomienie Policji o popełnieniu przestępstwa, wypełniając tym samym obowiązek o którym mowa w art. 44 ustawy.

Zgodnie z art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych 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. Zgodnie z art. 45 ust. 1 ww. ustawy ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika 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 autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazującej 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 z okoliczności sprawy wynika, że powód miał prawo być przekonany, iż komunikat pochodzi od banku, ponieważ był identyczny jak komunikaty dotychczas przez bank generowane, komunikat pojawił się po poprawnym zalogowaniu się powoda do serwisu transakcyjnego banku, próbował go dwukrotnie obejść, co wskazuje na okoliczność, iż nie podszedł do tej wiadomości bezrefleksyjnie, ale nieusuwalność komunikatu i każdorazowe pojawienie się przekonała go o jego wiarygodności. Nad to wiadomość sms została przesłana na numer telefonu podany przez powoda bankowi do autoryzacji transakcji. Wcześniej brak było jasnych komunikatów i ostrzeżeń ze strony banku do których z łatwością mógł dotrzeć powód ostrzegających o tych nieuczciwych i nielegalnych praktykach, w tym o cyberprzestępczości czy działaniu zorganizowanej grupy przestępczej wymuszającej potwierdzenie zabezpieczenia transakcji, co prowadzi do przechwycenia danych umożliwiających dostęp do konta klienta. Strona pozwana podnosiła, iż umieszczała na swoich stronach internetowych ostrzeżenia, jednak załączone wydruki nie wskazują w jakim konkretnie okresie były one widoczne na stronach internetowych, czy przede wszystkim obejmuje to okres przed przedmiotowym zdarzeniem, jakie dokładnie treści przekazywał bank. Jak zeznał świadek zawnioskowany przez stronę pozwaną o procederze, którego ofiarą jest powód, bank informował dwukrotnie, w zakładce aktualności. Jednocześnie jak zeznała żona powoda, bezpośrednio po stwierdzeniu kradzieży, przeglądali stronę internetową pozwanego banku i żadnych informacji ostrzegawczych nie znaleźli. Zdaniem sądu o wąskiej dostępności tych komunikatów, a tym samym nieskuteczności kampanii ostrzegawczej prowadzonej przez bank, jak i o nieodosobnionym przypadku powoda, świadczy ilość osób który w ten sam sposób przekazały swoje dane i doznali szkody na skutek tego przestępczego działania, o czym świadczą zeznania świadka zawnioskowanego przez bank, który potwierdził okoliczność zintensyfikowania kampanii phising po koniec maja 2015 roku, jak i skala prowadzonego postępowania karnego. Powód nie informował nikogo o swoim loginie ani haśle do konta. Nie korzystał z opcji zapamiętywania hasał. Był uczulony na sprawdzenie przez zalogowaniem się do bankowości internetowej czy połączenie jest szyfrowanego, o co uczulał również swoją małżonkę w przypadku korzystania przez nią z tego rodzaju usług banku. Ponad to powód logował się z komputera zainstalowanego w Instytucie (...) z komputera posiadającego legalne oprogramowanie oraz aktywny i aktualny program antywirusowy.

Z tych względów, zdaniem sądu, nieuzasadnione byłoby przyjęcie, zwalniające pozwany bank z odpowiedzialności, iż powód reagując na wyświetlony komunikat umyślnie doprowadził do nieautoryzowanej transakcji płatniczej bądź umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 ustawy. Pozwany nie wykazał w toku postępowania, by powód umyślnie czy wskutek rażącego

niedbalstwa naruszył któryś z obowiązków o których mowa w art. 42 ustawy, a w szczególności poprzez udostępnienie instrumentu płatniczego osobom nieuprawnionym, bowiem jego działanie które doprowadziło do zdefiniowania osoby na której zostały przelane środki z konta powoda nie było działaniem umyślnym, a niezamierzonym i nieświadomym, co wskazuje na niedbalstwo jednak w żadnym wypadku nie w stopniu rażącym.

Jednocześnie zdaniem sądu w oparciu o przepis art. 46 ust. 2 ww. ustawy zasadne było obniżenie należnej powodowi kwoty o równowartość kwoty 150 €, ustalonej przy zastosowaniu kursu średniego ogłoszonego przez NBP obowiązującego w dniu wykonania transakcji to jest z dnia 3 czerwca 2015 roku, gdzie kurs ten wynosił 4,1307 zł. (z dnia 4 czerwca 2015 roku brak notowań kursu NBP) Z treści art. 42 ust 2 ww. ustawy wynika, iż odpowiedzialność płatnika jest niezależna od jego winy i może być przypisana niezależnie od tego czy dopuścił się naruszenia w wyniku niedbalstwa.

O odsetkach sąd orzekł na podstawie art. 481 kc, zgodnie z żądaniem pozwu. Zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych, pozwany miał obowiązek niezwłocznego zwrotu kwoty nieautoryzowanych transakcji. Powód złożył reklamację w dniu 9 czerwca 2015 roku i pomimo dalszych pism do niego kierowanych, reklamacji do dnia dzisiejszego nie uwzględnił, tym samy mając na uwadze datę zgłoszenia reklamacji – 9 czerwca 2015 roku, żądanie odsetek od daty wskazanej w pozwie jest w ocenie sądu w pełni uzasadnione.

Z tych względów sąd orzekł jak w pkt I wyroku, oddalając powództwo w pozostałym zakresie to jest kwoty stanowiącej równowartość 150 €.

O kosztach postępowania sąd orzekł na podstawie art. 98 kpc, przy przyjęciu, iż powód wygrał proces w 99%. Na koszty postępowania składają się opłata od pozwu i wynagrodzenie pełnomocników.

SSO Ewa Ligoń-Krawczyk