Sygn. akt II C 73/16

UZASADNIENIE

Pozwem z dnia 4 grudnia 2015 r. K. M. wystąpił przeciwko (...) Spółce Akcyjnej z siedzibą w W. o orzeczenie nakazem zapłaty wydanym w postępowaniu upominawczym, aby pozwany Bank zapłacił na jego rzecz kwotę 86.860 zł wraz z ustawowymi odsetkami od dnia 24 grudnia 2013 r. do dnia zapłaty oraz koszty postępowania, w tym koszty zastępstwa radcowskiego według norm przepisanych. (pozew – k. 2-11)

Nakazem zapłaty z dnia 30 grudnia 2015 r. wydanym w postępowaniu upominawczym, Sąd Okręgowy w Łodzi, w sprawie II Nc 306/15, orzekł zgodnie z żądaniem pozwu. (nakaz zapłaty – k. 125)

W sprzeciwie od nakazu zapłaty z dnia 25 stycznia 2016 r. strona pozwana wniosła o oddalenie powództwa w całości oraz o zasądzenie od powoda kosztów zastępstwa procesowego w wysokości 2-krotności stawki minimalnej oraz 17 zł tytułem opłaty skarbowej od pełnomocnictwa. Podniosła zarzut przyczynienia się powoda do powstania szkody w 100% oraz zarzut potrącenia. (sprzeciw – k. 130-134)

Sąd Okręgowy ustalił następujący stan faktyczny:

W dniach 20 sierpnia 2003 r. i 5 kwietnia 2012 r. K. M. zawarł z (...) Bank Spółką Akcyjną z siedzibą w W. dwie umowy o prowadzenie bankowych rachunków: bieżącego oraz oszczędnościowo-rozliczeniowego, na podstawie, których otwarty został internetowy rachunek o nr (...) oraz rachunek (...) nr (...). (umowa – k. 174-178, umowa – k. 111-113, potwierdzenie otwarcia rachunku – k. 114)

W dniu 11.04.2013 r. aktem notarialnym Rep. A nr (...) sporządzonym przez Notariusza w W. T. C., zmieniono m.in. § 1 i § 2 Statutu pozwanego, w wyniku czego, z dniem wpisu ww. zmiany do Krajowego Rejestru Sądowego, zmianie uległa nazwa pozwanego z (...) Bank S.A. na (...) S.A. (odpis pełny z KRS pozwanego – k. 17-46)

W dniach 6 i 9 grudnia 2013 r. niezidentyfikowany sprawca wykonał, bez wiedzy i zgody powoda, operacje bankowe na rachunku o nr (...): przelewu wewnętrznego przychodzącego z rachunku powoda (...)nr (...) w kwocie 95.000 zł, a następnie przelewów zewnętrznych wychodzących typu (...) na rachunek K. S. o nr (...) w kwotach 29.610 zł, 29.720 zł, 27.530 zł, 26.384 zł, 27.000 zł. (potwierdzenia przelewów – k. 53-58)

Przed wykonaniem tych operacji, powód w dniu 6 grudnia 2013 r. o godz. 12:00:33 zalogował się w serwisie internetowym (...) z komputera stacjonarnego znajdującego się w jego biurze, na którym zainstalowane było oprogramowanie antywirusowe (...) z automatyczną aktualizacją bazy. Do komputera miał dostęp tylko i wyłącznie powód, który uruchamiał komputer poprzez wpisanie hasła. W celu zalogowania się na stronie (...), powód ręcznie wpisał w wyszukiwarce stronę pozwanego, następnie otworzył stronę banku, przeszedł na ikonę logowania, otworzyło się okno logowania, powód wpisał identyfikator (login) i stałe hasło ustanowione przez niego. Po prawidłowym zalogowaniu do serwisu transakcyjnego, pojawiła się informacja o rebrandingu, zmianie nazwy banku oraz połączeniu, co wiązało się z przedefiniowaniem obecnych numerów rachunków bankowych na nowe. W tle widoczna była rzeczywista strona banku wraz z właściwymi saldami rachunków bankowych. Komunikat wymagał potwierdzenia. Powód nie mógł wylogować się z serwisu transakcyjnego, dopóki nie zatwierdził komunikatu. W tym czasie tj. o godz. 12:01:53 powód otrzymał wiadomość sms z banku o treści: „Operacja nr 1 z dnia 06-12-2013 Definicja odbiorcy z rach.: (...) na rach.: (...), hasło: (...)", które następnie wpisał i zatwierdził komunikat. Wtedy przeszedł na stronę serwisu transakcyjnego i wylogował się. Do dnia 9 grudnia 2013 r. powód nie korzystał z bankowości elektronicznej. Nie miał wiedzy o dokonywanych przelewach między 6 grudnia a 9 grudnia 2013 r. (pismo – k. 310-313, zeznania powoda – e-protokół k. 526 v.-528, adnotacja 00:20:00, opinia biegłego informatyka – k. 453)

K. M. nie podał nikomu loginu i hasła do swojego konta w (...). Powód czytał komunikaty dotyczące bezpieczeństwa pojawiające się na stronie Banku. (zeznania powoda – e-protokół, k. 526 v.-528, adnotacja 00:20:00)

Przed zdarzeniami z dnia 6 grudnia 2013 r. mBank nie informował swoich klientów o zagrożeniach zawiązanych z komunikatem dotyczącym połączenia banków, rebrandingu i przedefiniowania obecnych numerów rachunków bankowych na nowe. (zeznania powoda – e-protokół, k. 526 v.-528, adnotacja 00:20:00)

W dniu 9 grudnia 2013 r. powód zalogował się na konto i stwierdził na nim brak środków. Powód zauważył kilka przelewów na duże kwoty, których nie wykonywał. (zeznania powoda – e-protokół, k. 526 v.-528, adnotacja 00:20:00)

Powód ani nikt przez niego upoważniony nie zlecił i nie autoryzował tych przelewów, nie udostępnił nikomu danych umożliwiających zalogowanie się na konto drogą elektroniczną i dokonanie przelewów. Osoba będąca odbiorcą przelewów – K. S. nie była znana K. M.. (zeznania powoda – e-protokół, k. 526 v.-528, adnotacja 00:20:00)

W dniu 9 grudnia 2013 r. powód poprzez infolinię złożył pozwanemu reklamację dotyczącą nieautoryzowanych przelewów i dyspozycję zwrotu kwot nieautoryzowanych transakcji. Reklamacja powoda została zarejestrowana tego samego dnia pod numerem (...). Po złożeniu reklamacji z powodem skontaktował się pracownik pozwanego Banku (...). Reklamacja powoda nie została uwzględniona. (zeznania powoda – e-protokół, k. 526 v.-528, adnotacja 00:20:00, wydruk – k.66, korespondencja e-mail – k. 59-107)

W tym samym dniu powód zawiadomił Komisariat Policji w G. - R. o kradzieży pieniędzy w kwocie 95.000 zł z jego rachunków bankowych o nr (...) i (...) nr (...) prowadzonych przez pozwanego. Sprawa została zarejestrowana pod sygnaturą akt 70796/2013. Ostatecznie sprawę przekazano do Prokuratury Okręgowej w Olsztynie za oznaczeniem V ds. 14/14. (okoliczność bezsporna)

W dniu 9 grudnia 2013 r. dokonano z rachunku K. S. o nr (...) zwrotu środków w wysokości 27.000 zł oraz 26.384 zł na rachunek bankowy powoda o nr (...). (potwierdzenie przelewów z dnia 9 grudnia 2013 r. – k. 51-52)

Ostatecznie z rachunku bankowego powoda wyprowadzono łączną kwotę 86.860 zł. (potwierdzenie przelewów z dnia 9 grudnia 2013 r. – k. 51-58)

Klient pozwanego (...) logując się z komputera do systemu bankowości elektronicznej musi dokonać autoryzacji za pomocą loginu, czyli ID przypisanego do użytkownika nadawanego przez Bank i statycznego hasła, znanego tylko klientowi. Bank nie zna hasła klienta. W bazach Banku przechowywany jest skrót z hasła, na podstawie, którego Bank stwierdza, czy wpisywane hasło jest prawidłowe. Hasło statyczne, oznacza, że jest ono niezmienne dopóki użytkownik go nie zmieni. Logując się do systemu użytkownik wpisuje całe hasło, nie jest ono maskowane. Hasło maskowane oznacza, że przy logowaniu wpisywane są tylko niektóre pozycje z hasła. Przelew środków na rachunek innego użytkownika wymaga autoryzacji transakcji dokonywanej zależnie od metody autoryzacji wybranej przez użytkownika: poprzez kod wysyłany sms-em lub kod z papierowej karty dostarczanej użytkownikowi. W przypadku przelewów wewnętrznych pomiędzy rachunkami bankowymi klienta prowadzonymi przez pozwanego oraz przelewów dokonywanych na rzecz zdefiniowanego odbiorcy zaufanego niewymagana jest autoryzacja operacji poprzez jej potwierdzanie jednorazowym hasłem. (zeznania świadka T. W. – e-protokół k. 430 v.-432, adnotacja 00:09:49, 00:26:38)

Struktura tworzenia zdefiniowanego odbiorcy zaufanego w (...) jest elementem pozwalającym użytkownikowi stworzyć odbiorcę w systemie, któremu przekazywanie środków nie generuje konieczności potwierdzania tych operacji hasłami sms. Raz zdefiniowany odbiorca i zatwierdzony hasłem sms jest już w systemie zdefiniowanym kontem, na które można przelewać środki o nieograniczonej ilości bez dodatkowych uwierzytelnień. Powód myśląc, że wykonuje polecenie Banku w zakresie zmiany numeru rachunku bankowego, w rzeczywistości zdefiniował nowego odbiorcę o nr konta (...). (opinia biegłego informatyka – k. 455)

Pojawiający się komunikat po zalogowaniu do serwisu transakcyjnego, blokował dostęp do dalszych czynności dokonywanych na rachunku bankowym. Inicjował wysyłanie przez bank wiadomości sms z hasłem jednorazowym, a w tym przypadku było to dodanie zdefiniowanego odbiorcy zaufanego. Atak polegał na podstawieniu danych niewidocznych dla klienta, potrzebnych do wykonania przelewu zdefiniowanego. Dla użytkownika z komunikatu

wynikało, że odbiorcę należy zdefiniować ze względu na reorganizację banku. (zeznania świadka T. W. – e-protokół k. 430 v.-432, adnotacja 00:09:49, 00:26:38)

Na twardym dysku jednostki centralnej komputera klasy PC, należącego do powoda, ujawniono oprogramowanie szpiegujące służące do uzyskiwania danych w postaci złośliwego oprogramowania o nazwie (...) umożliwiającego zdalną instalację oprogramowania przy jednoczesnej dezaktywacji oprogramowania antywirusowego zainstalowanego na atakowanym komputerze oraz program (...)dedykowany do ataków na komputery użytkowników wykorzystujących systemy bankowości internetowej i umożliwiający przejęcie pełnej kontroli nad zainfekowanym komputerem oraz uzyskania dostępu do rachunku bankowego ofiary. W czasie ataku przy logowaniu do serwisu transakcyjnego oprogramowanie wirusowe przechwytuje identyfikator i hasło klienta, następnie wyświetla komunikat o „łączeniu banków" wymagając przy tym podania hasła jednorazowego. Klient wprowadzając hasło jednorazowe w rzeczywistości ustanawia zdefiniowanego odbiorcę zaufanego – przelewy do niego nie wymagają dodatkowego potwierdzenia hasłem jednorazowym.

Dane konieczne do wykonania operacji na rachunku bankowym powoda – login i hasło, zostały wykradzione bezpośrednio od powoda. Jedynym zabezpieczeniem pozwanego mogło być stosowane przez bank oprogramowanie antyfraudowe, jednakże według ówcześnie zdefiniowanych reguł mogło ono nie wychwycić transakcji na rachunku powoda, oznaczonych, jako podejrzane do weryfikacji przez pracowników Banku. System antyfraudowy nigdy nie definiował w strukturze banku utworzenia zdefiniowanego odbiorcy zaufanego, jako alertu, gdyż nie jest to operacja związana z transferem gotówki. Podział kwot upłynnionych z rachunku powoda był odpowiednio przewidziany by nie przekroczyć kwoty 15.000 euro, żeby nie poddać transakcji badaniu antyfraudowemu. Działanie złośliwego oprogramowania było przezroczyste i mogło nie wykazywać żadnych symptomów utrudniających pracę komputera powoda.

Model funkcjonowania polegającego na przejęciu danych logowania do konta użytkownika wraz z wytworzoną socjotechniką i przygotowanym sztabem tzw. mułów, którzy to odbiorą pieniądze z bankomatu i wpłacą na zlecone konta pod pewnym pretekstem wymyślonym przez niby pracodawców, funkcjonuje w kubaturze światowego Internetu i ataków na konta bankowe na całym świecie od 2007 roku. Ta metoda działania została określona, jako phishing i pojawia się systematycznie. Jest agresywnie wykorzystywana w momentach gdzie hakerzy wiedzą o zbliżającym się zamieszaniu, zmianach organizacyjnych w jednostkach banków. Trzy transakcje zostały wykonane w piątek, w godzinach przed 15:00, gdzie dokonywanie transakcji przelewów (...) można realizować jedynie do godziny 15:00. Dodatkowo, było to już na koniec dnia transakcyjnego oraz przed weekendem. Pracownicy etatowi banków z obydwu stron transakcji mogli być mniej wyczuleni na tego typu transakcje w formie weryfikacji antyfraudowej. Hakerzy wykorzystali dodatkowo, jako zabezpieczenie dla zniwelowania potencjalnego zablokowania transakcji ciąg przelewów o niższych nominałach (poniżej 15 000 Euro), aby nie podlegały one weryfikacji „z klucza" - zgodnie z ustawą z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (Dz.U. z 2003 r. Nr 153, poz. 1505 z późn. zm.). Transakcje na rachunku K. M. na przestrzeni niedużego okresu czasu były dość zintensyfikowane oraz o nominałach przewyższających standardowe transakcje na koncie powoda, co mogło wzbudzić reakcję systemu antyfraudowego, ale też system mógł nie zostać tymi operacjami zaniepokojony i przepuścił realizację transakcji dalej. Dodatkowo był to koniec tygodnia, a system antyfraudowy jest skorelowany z reakcją pracownika, który musiałby podjąć akcję w tym zakresie. System antyfraudowy w grudniu 2013 roku był obsługiwany przez pracowników etatowych (...), którzy pracowali w systemie jednozmianowym w godzinach 9 – 17. Dopiero od 2015 roku w (...) wprowadzono system monitoringu antyfraudowego 24/7 tj. nadzoru całodobowego. (opinia biegłego informatyka – k. 447-464,496 – 507, pismo – k. 310-313)

Pismem z dnia 16 czerwca 2014 r. powód wezwał pozwany Bank do zapłaty na jego rzecz wartości środków finansowych przekazanych osobom nieuprawnionym z jego rachunku bankowego w terminie do 23 czerwca 2014 r. (pismo powoda – k. 47-49)

Postanowieniem Prokuratora Okręgowego w Olsztynie z dnia 16 grudnia 2015 r. zawieszone zostało śledztwo V ds. 14/14 w sprawie przejęcia na rachunki bankowe środków pieniężnych pochodzących z korzyści związanych z popełnieniem czynu zabronionego, tj. o przestępstwo z art. 299 § 1 k.k. Tok dalszego postępowania zależy od wyników czynności wykonywanych w ramach międzynarodowej pomocy prawnej. (postanowienie – k. 191-194)

Powyższy stan faktyczny Sąd ustalił na podstawie zeznań powoda i świadka, dokumentów znajdujących się w aktach niniejszej sprawy. W zakresie wiadomości specjalnych Sąd oparł się na opinii biegłego sądowego z zakresu informatyki, który udzielił wyczerpujących wyjaśnień na temat rodzaju i jakości zabezpieczeń elektronicznych stosowanych przez pozwanego w dniu 6 grudnia 2013 r. w stosunku do rachunków bankowych powoda, możliwości przełamania tych zabezpieczeń, możliwości zainstalowania oprogramowania szpiegowskiego i ataku hakerskiego na komputerze powoda.

Sąd Okręgowy zważył, co następuje:

Zgodnie z art. 725 k.c. przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych.

Zapewnienie bezpieczeństwa depozytów jest jednym z najistotniejszych obowiązków banku, a sposób jego wykonywania jest najbardziej wymierną podstawą oceny jego wiarygodności, w związku z czym wszelkie próby interpretacji przez banki postanowień zawartych w stosowanych przez nie wzorcach umownych, zmierzające do zaniżania standardów bezpieczeństwa powierzonych bankowi środków pieniężnych, powinny być oceniane, jako zachowania sprzeczne z dobrymi obyczajami i celem umowy rachunku bankowego (SN w wyr. z 14.4.2003 I CKN 308/61).

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 r. Ustawa ta przewiduje generalną zasadę zgodnie, z którą dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika. Stosownie do 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 transakcją płatnicza. Art. 45 ust. 1 powołanej ustawy stanowi, że 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 (art. 45 ust. 2 ustawy o usługach płatniczych).

Zobowiązanie banku, jako profesjonalnego podmiotu jest determinowane poprzez ustawowe obowiązki wskazane m.in. w art. 43 ust. 1 ustawy o usługach płatniczych. Pozwany mBank nie wywiązał się z ich wypełnienia w stosunku do powoda. W szczególności nie zapewnił, by indywidualne zabezpieczenia instrumentu płatniczego nie były dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Gdyby, bowiem zabezpieczenia transakcji elektronicznych stosowane przez pozwanego były właściwe, nie doszłoby do dokonania na rachunku powoda transakcji przez nieuprawnione do tego osoby. Wprawdzie w grudniu 2013 roku pozwany korzystał z oprogramowania antyfraudowego, lecz nie wychwyciło ono nietypowych operacji na rachunku powoda, bądź nie zrobił tego pracownik (...). O możliwości wychwycenia nieprawidłowości świadczy najlepiej to, iż zostały one zauważone przez pracowników (...) Oddział w Ł.. Należy dodać, co wiadomo Sądowi z urzędu, że takich przypadków jak powoda było w pozwanym Banku znacznie więcej, co wskazuje, że zabezpieczenia stosowane przez pozwanego nie były właściwe.

Zobowiązanie Banku względem posiadacza rachunku kształtuje również art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (tekst jednolity Dz.U. Nr 72 z 2002 r., poz. 665 ze zmianami), który stanowi, iż bank jest zobowiązany do dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. W ocenie Sądu w niniejszym przypadku mBank nie dołożył szczególnej staranności w tym zakresie, dopiero, bowiem w 2015 roku wprowadzono system monitoringu antyfraudowego całodobowego.

Należy wskazać, że zgodnie z art. 46 ust. 3 ustawy o usługach płatniczych, płatnik (w niniejszym przypadku powód) odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia, co najmniej jednego z obowiązków, o których mowa w art. 42.

W ocenie Sądu powód, jako klient banku nie naruszył obowiązków, o których mowa w art. 42 umyślnie lub wskutek rażącego niedbalstwa. Wskazać należy, iż powoda nie wiążą te postanowienia Regulaminu otwierania i prowadzenia rachunków oszczędnościowych - rozliczeniowych i bieżących w (...), które są dla niego mniej korzystne niż przepisy ustawy o usługach płatniczych. Zgodnie, bowiem z treścią art. 8 ust. 1 i 2 ustawy o usługach płatniczych „postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego nie mogą być mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy, chyba, że ustawa stanowi inaczej. Postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy są nieważne, zamiast nich stosuje się odpowiednie przepisy ustawy". Wprowadzenie przez pozwany Bank mniej korzystnych dla klienta regulacji niż ustawowe stanowi naruszenie art. 8 ust. 1 ustawy o usługach płatniczych, prowadząc do nieważności regulaminowych postanowień, na które powołuje się pozwany w sprzeciwie.

Zdaniem Sądu powodowi nie można przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa. Komputer powoda posiadał zainstalowane oprogramowanie antywirusowe i nie przejawiał żadnych problemów z funkcjonowaniem czy zainfekowaniem oprogramowaniem wirusowym, nadto był chroniony hasłem zabezpieczającym dostęp osobom trzecim. W ocenie Sądu, potwierdzenie przez powoda wyświetlonego podczas logowania na stronę (...), komunikatu informującego o połączeniu instytucji bankowych i przedefiniowaniu w związku z tym numerów kont, które spowodowało w dalszej kolejności przejęcie przez szkodliwe oprogramowanie loginu, hasła oraz ustanowienie zdefiniowanego odbiorcy zaufanego, nie nosi cech rażącego niedbalstwa. Powód miał prawo pozostawać w przekonaniu, że komunikat wyświetlający się podczas logowania na stronę Banku pochodzi właśnie od (...) i służy zmianie dotychczasowego numeru konta na nowe. Komunikat mówiący o potrzebie zmiany rachunku bankowego pojawił się po wpisaniu adresu prawdziwej strony (...) i zalogowaniu do serwisu transakcyjnego. Komunikat zajmował część strony, na której widniało prawidłowe saldo. Był też widoczny symbol zamkniętej kłódki oznaczający bezpieczną stronę. Pozwany nie ostrzegał w dacie zdarzenia swoich klientów przed tego rodzaju komunikatami, nie informował, iż skorzystanie z nich może nieść za sobą negatywne skutki. Należy podkreślić, że powód nie przekazał osobom trzecim swojego loginu ani hasła do konta bankowego, a zatwierdzając komunikat nie był w stanie stwierdzić, iż ustanowił zdefiniowanego odbiorcę zaufanego w osobie K. S., gdyż nie widział danych umożliwiających dokonanie takowej operacji. Należy podkreślić, że przepis art. 46 ustawy o usługach płatniczych jest przepisem szczególnym, regulującym odpowiedzialność Banku (zwanego dostawcą płatnika) w przypadku wystąpienia nieautoryzowanej transakcji płatniczej. Odpowiedzialność Banku za taką transakcję jest uchylona w razie doprowadzenia do nieautoryzowanej transakcji przez klienta w sposób umyślny lub wskutek umyślnego albo stanowiącego rażące niedbalstwo naruszenia obowiązków, o których mowa w art. 42. W sytuacji określonej w art. 46 ust. 2 (m.in. naruszenia obowiązku, o którym mowa w art. 42 ust. 2, nienoszącego cech umyślności ani rażącego niedbalstwa) płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 150 euro. W niniejszej sprawie nie znajduje zastosowania ani ust. 2, ani ust. 3 art. 46, powód, bowiem nie naruszył obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych. Bezzasadne jest tym samym twierdzenie pozwanego, że powód przyczynił się do powstania szkody. Należy dodać, iż powód spełnił wynikający z art. 42 ust. 1 pkt. 2 ustawy o usługach płatniczych obowiązek niezwłocznego zawiadomienia o zaistnieniu nieautoryzowanej transakcji płatniczej.

W związku z powyższym, zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych, pozwany jest zobowiązany niezwłocznie zwrócić powodowi kwotę nieautoryzowanych transakcji płatniczych, która łącznie wyniosła 86.860 zł.

Dodać należy, iż całkowicie bezzasadny był zarzut potrącenia zgłoszony przez pozwanego. Pozwany nie wskazał, ani nie udowodnił jaką to wierzytelność posiada wobec powoda, nie wskazał także jaka jest wysokość rzekomej wierzytelności, którą chciałby potrącić.

W zakresie żądania zasądzenia odsetek Sąd zważył, iż stosownie do przepisu art. 481 § 1 k.c., jeżeli dłużnik opóźnia się ze spełnieniem świadczenia, wierzyciel może żądać odsetek za czas opóźnienia, choćby nie poniósł żadnej szkody i chociażby opóźnienie było następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi. Zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych, pozwany miał obowiązek niezwłocznego zwrotu kwoty nieautoryzowanych transakcji. Przyjmuje się, iż termin „niezwłocznie" oznacza termin realny, mający na względzie okoliczności miejsca i czasu. Zdaniem Sądu żądanie odsetek od kwoty 86.860 zł w terminie 14 dni od dnia złożenia przez powoda reklamacji co do kwot nieautoryzowanych transakcji jest zasadne w okolicznościach sprawy. Powód, bowiem złożył dyspozycję wypłaty kwot w dniu 9 grudnia 2013 r. Od dnia 1 stycznia 2016 r. powodowi należą się odsetki ustawowe za opóźnienie, zgodnie z aktualnym brzmieniem art. 481 k.c.

Sąd orzekł o kosztach procesu na podstawie art. 98 k.p.c., zasądzając od pozwanego na rzecz K. M. kwotę 5.102,85 zł stanowiącą koszty poniesione przez powoda w toku procesu. Na kwotę tą złożyły się: 1000 zł opłaty sądowej, 3600 zł tytułem wynagrodzenia pełnomocnika (ustalonego na podstawie § 6 ust. 6 rozporządzenia Ministra Sprawiedliwości z dnia 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 (Dz.U.2013.490 j.t.), 17 zł tytułem opłaty skarbowej od pełnomocnictwa oraz 485,85 zł kosztów wynagrodzenia biegłego.

O zwrocie na rzecz stron niewykorzystanych zaliczek na poczet wynagrodzenia biegłego /punkt 2 i 3b wyroku/ Sąd orzekł na podstawie art. 84 ust. 1 w/w ustawy o kosztach sądowych w sprawach cywilnych.

Na podstawie art. 80 ust. 1 ustawy o kosztach sądowych w sprawach cywilnych, Sąd rozstrzygnął o zwrocie na rzecz powoda nadpłaconej opłaty sądowej /punkt 3a wyroku/.