Sygn. akt III C 918/15

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

dnia 09 stycznia 2017 rok

Sąd Okręgowy w Warszawie III Wydział Cywilny

w składzie:

Przewodniczący:	SSO Mariusz Solka
Protokolant:	Sekretarz sądowy Tamara Oktaba

po rozpoznaniu w dniu 05 stycznia 2017 roku w Warszawie

na rozprawie

sprawy z powództwa A. K.

przeciwko pozwanemu (...) Bank (...) S.A. w W.;

o zapłatę

orzeka:

1. powództwo oddala;

2. zasądza od powoda A. K. na rzecz pozwanego (...) Bank (...) S.A. w W., kwotę 4.608,07 (cztery tysiące, sześćset osiem, 07/100) złotych kosztów procesu, w tym kwotę 3.600,00 (trzy tysiące, sześćset) złotych tytułem wynagrodzenia pełnomocnika;

3. nakazuje pobrać od powoda A. K. na rzecz Skarbu Państwa –Sądu Okręgowego w Warszawie, kwotę 1.422,67 (jeden tysiąc, czterysta dwadzieścia dwa, 67/100) złotych tytułem wydatków pokrytych tymczasowo przez Skarb Państwa.---

/-/ SSO Mariusz Solka

Sygn. akt ***III C 918/15***

UZASADNIENIE

Powód A. K. wystąpił w dniu 21 lipca 2015 r. z pozwem przeciwko (...) Bank (...) Spółce akcyjnej w W., którym domagał się orzeczenia nakazem zapłaty w postępowaniu nakazowym, że pozwany ma zapłacić na rzecz powoda kwotę 137.665 zł wraz z odsetkami ustawowymi od dnia 29 maja 2015 r. do dnia zapłaty wraz z kosztami opłaty sądowej według norm przepisanych, kosztami opłaty skarbowej od pełnomocnictwa w kwocie 17 zł i kosztami zastępstwa procesowego w kwocie 7.200 zł. W uzasadnieniu pozwu wskazał, że strony łączy umowa rachunku bankowego, z którego w dniu 28 maja 2015 r. pozwany bez zlecenia, wiedzy i zgody powoda dokonał siedmiu przelewów na rachunek bankowy o numerze (...), przynależny do P. O., na łączną kwotę 137.285 zł oraz obciążył powoda w związku z tym opłatami

w kwocie 280 zł. Powód zgłosił pozwanemu nieautoryzowane przelewy i wniósł o zwrot kwoty 137.665 zł, którego żądania pozwany nie uwzględnił. (pozew k. 3-6)

Zarządzeniem z dnia 7 sierpnia 2015 r. stwierdzono brak podstaw do wydania nakazu zapłaty w postępowaniu nakazowym i w postępowaniu upominawczym. (zarządzenie k. 50)

Pozwany w odpowiedzi na pozew wniósł o oddalenie powództwa oraz o zasądzenie od powoda na rzecz pozwanego zwrotu kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych. Pozwany podniósł, że sporne przelewy zostały zlecone po poprawnym zalogowaniu w serwisie (...) numerem klienta oraz hasłem dostępu oraz zrealizowane w oparciu o szablon płatności prawidłowo aktywowany przy pomocy jednorazowego kodu aktywacyjnego pochodzącego z karty kodów przypisanej do powoda. Pozwany przeprowadził weryfikację przelewów w granicach jego możliwości. Pozwany wskazał, iż Bank informował na swojej stronie internetowej umożliwiającej dostęp do bankowości elektronicznej o danych niezbędnych do poprawnego zalogowania oraz wymaganiach systemowych w celu zapewnienia korzystającym bezpieczeństwa w używaniu tej formy bankowości. Pozwany, odwołując się do nieuwzględnionej reklamacji, podniósł, że nie ponosi odpowiedzialności za brak staranności powoda w kontekście dbałości o własne interesy finansowe. Brak dbałości wywodzi z zaniechania zabezpieczenia systemu informatycznego wykorzystywanego przez powoda w sposób wymagany do uniknięcia zainfekowania wirusem, a także z niezachowania należytej staranności w sytuacji żądania od niego czynności nietypowej, polegającej na podaniu jednorazowego kodu aktywacyjnego, w sytuacji, gdy klient był wielokrotnie informowany o tym, że bank nigdy nie żąda podania tych kodów podczas logowania. Pozwany wywodził, iż powód nie wykazał szkody w zakresie zwrotu całości przelanych środków przez beneficjenta przelewów. (odpowiedź na pozew k. 59-71v)

Powód w replice na odpowiedź na pozew wskazał, że co najmniej na kilka miesięcy przed nieautoryzowaną dyspozycją przestał korzystać z kodów z karty jednorazowych na rzecz autoryzacji w formie smsów oraz, że logując się do systemu bankowości elektronicznej zawsze korzystał ze sprzętu przestrzegając zasad bezpieczeństwa, tj. posiadając legalne i aktualne oprogramowanie w tym antywirusowe oraz zaporę firewall, aktualizowaną regularnie przeglądarkę internetową oraz nigdy nie korzystał z żadnych stron podobnych do strony banku. Zaprzeczył, aby reagował na nietypowe prośby o podanie kodu narzędzia autoryzacyjnego. Podniósł, że sprawca musiał wiedzieć o limitach ustanowionych na rachunku powoda ustalonych na kwotę 20.000 zł. Zarzucił, że pozwany nie posiada sprawnego systemu monitoringu nietypowych transakcji, co doprowadziło do wyprowadzenia z rachunku bankowego powoda w ciągu kliku minut dumy siedmiokrotnie przewyższającej ustalony limit. (replika k. 145-151).

W piśmie procesowym z dnia 21 kwietnia 2016 roku, pozwany przyznał, iż powód do autoryzacji transakcji w serwisie internetowym korzystał z kodów jednorazowych przysłanych w wiadomościach SMS na wskazany przez powoda numer telefonu (k. 221-226).

Sąd Okręgowy ustalił następujący stan faktyczny:

A. K. jest klientem (...) (...) Banku (...) S.A. w W. (dalej: (...) S.A.) i posiada w tym banku dwa rachunki bankowe, tj. indywidualny o numerze (...) oraz firmowy o numerze (...). (dowód: okoliczności bezsporne)

A. K. zawarł w dniu 22 marca 2006 r. (...) S.A. umowę rachunku oszczędnościowo-rozliczeniowego P., na mocy której bank zobowiązał się do otwarcia i prowadzenia rachunku oszczędnościowo-rozliczeniowego o numerze (...) na rzecz posiadacza rachunku oraz świadczenia na rzecz posiadacza rachunku kompleksowej indywidualnej obsługi w ramach programu bankowości prywatnej P. i zapewnienia najwyższej staranności w realizacji wszelkich spraw posiadacza rachunku wynikających ze współpracy z (...) S.A. (§ 1 umowy). Z tytułu prowadzenia kompleksowej obsługi w ramach pakietu P. bank był uprawniony do pobierania od posiadacza miesięczną opłatę tzw. „opłatę pakietową", która obejmowała (§ 9 ust. 1 umowy) oraz prowizje oraz opłaty w wysokości określonej w Taryfie prowizji i opłat bankowych w (...) SA w części, w której usługi nie są objęte opłatą pakietową (§ 10 ust. 1 umowy). Za realizację wysokokwotowych zleceń na rachunki prowadzone w innych niż (...) S.A. bankach za pośrednictwem systemu (...) w kwocie niższej niż 1 mln zł (...) S.A. w dniu zawarcia umowy pobierał opłatę w kwocie 35 zł. (dowód: umowa rachunku

oszczędnościowo-rozliczeniowego P. wraz z załącznikami nr 1 i 2 k. 17-24, wyciąg z Taryfy prowizji i opłat bankowych k. 21-24)

W dniu 30 czerwca 2011 r. strony zmieniły powyższą umowę na umowę rachunku oszczędnościowo-rozliczeniowego Konto P. (...), usług bankowości elektronicznej oraz karty debetowej bez (...). A. K. przypisano numer klienta (...). Bank został upoważniony do pobierania prowizji i opłat bankowych za świadczenie usług, w tym prowadzenie rachunku, zgodnie z Taryfą prowizji i opłat bankowych w (...) Banku (...) SA (§8 ust. 1). Posiadacz uzyskał dostęp w ramach usług bankowości elektronicznej (...) Bank (...) SA do swoich rachunków i korzystania z usług bankowości elektronicznej, na zasadach określonych w umowie i Regulaminie (§ 1 pkt 3 umowy). W Regulaminie świadczenia usług bankowości elektronicznej w (...) Banku (...) SA wydanym w 2015 r. określono m.in. zasady składania dyspozycji za pośrednictwem elektronicznych kanałów dostępu oraz bezpiecznego dostępu do systemu. Określono dostęp do usługi bankowości elektronicznej za pośrednictwem strony internetowej www.pkobp.pl, który uzależniono od posiadania przez użytkownika - klienta urządzeń oprogramowania spełniającego wymagania techniczne, które (...) Bank (...) S.A. podaje do wiadomości klientów na stronie internetowej oraz w serwisie telefonicznym (§ 3 Regulaminu). Bank ustalił zasady autoryzacji zleceń w serwisie internetowym wskazując, że uznaje dyspozycję za autoryzowaną z chwilą jej potwierdzenia odpowiednio przez składającego dyspozycje klienta albo ustanowionego użytkownika (§ 9 ust. 2 Regulaminu). Klient został uprawniony do składania dyspozycji za pośrednictwem elektronicznych kanałów dostępu przez całą dobę z wyłączeniem okresu przerw niezbędnych do konserwacji, napraw technicznych lub przywrócenia poprawności funkcjonowania elektronicznych kanałów dostępu (§ 10 Regulaminu). Na mocy § 12 Regulaminu klient został zobowiązany do logowania oraz wykonywania dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście z użyciem instrumentów uwierzytelniających oraz do zachowania w tajemnicy informacji zapewniających bezpieczne korzystania z usług bankowości elektronicznej, w tym informacji przekazywanych bankowi dla celów weryfikacji oraz nieudostępniania i nieujawniania innym osobom instrumentów uwierzytelniających (tj. rozwiązań technologicznych lub danych służących do powiązania danej dyspozycji ze składającym ją klientem lub działającym w jego imieniu użytkownikiem w elektronicznych kanałach dostępu) (§ 12 ust. 1 i 2). Klient został zobowiązany do należytego zabezpieczenia urządzeń i oprogramowania, którymi posługuje się w celu korzystania z usług bankowości elektronicznej poprzez stosowanie wyłącznie legalnego oprogramowania, jego bieżącej aktualizacji i instalacji poprawek systemowych zgodnie z zaleceniami producentów, aktualnego oprogramowania antywirusowego i antyspamowego oraz zapory firewall, najnowszych wersji przeglądarek internetowych, haseł zabezpieczających przed nieuprawnionym dostępem do komputera osób trzecich (§ 12 ust. 3). Szczegółowy opis środków, jakie powinien przedsięwziąć klient w celu zapewnienia bezpieczeństwa dostępu do usług bankowości elektronicznej podawany jest do wiadomości klientów i użytkowników na stronie internetowej oraz w serwisie telefonicznym (§ 12 ust. 4). W § 13 ust. 1 Regulaminu zobowiązano klienta do niezwłocznego zgłoszenia utraty, kradzieży, przywłaszczenia, nieuprawnionego użycia albo zniszczenia instrumentów uwierzytelniających bądź nieuprawnionego dostępu do usług bankowości elektronicznej. Na wypadek wystąpienia nieautoryzowanych transakcji płatniczych, w § 14 Regulaminu ustalono, że (...) S.A. jest obowiązany niezwłocznie zwrócić klientowi kwotę nieautoryzowanej transakcji płatniczej albo przywrócić rachunek klienta do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza, chyba że klient uchybił terminowi zgłoszenia, tj. bez zbędnej zwłoki, nie później niż w terminie 13 miesięcy od dnia realizacji transakcji płatniczej albo do dnia, w którym niewykonana transakcja płatnicza miała być zrealizowana. Klienta obciążają jednak w pełnej wysokości nieautoryzowane transakcje płatnicze, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia, co najmniej jednego z obowiązków określonych w § 12 ust. 1 -3 oraz § 13 ust. 1. Od momentu zgłoszenia dokonanego przez klienta (...) SA przejmuje odpowiedzialność za zobowiązania finansowe powstałe w wyniku nieautoryzowanych transakcji płatniczych, chyba że klient doprowadził do nich umyślnie (§ 14 ust. 5 Regulaminu). Odpowiedzialność banku obejmuje również opłaty i prowizje, którymi został obciążony klient w rezultacie niewykonania lub nienależytego wykonania transakcji płatniczej (§ 14 ust. 6 Regulaminu). (dowód: umowa k. 78-84, Regulamin świadczenia usług bankowości elektronicznej w (...) Banku (...) SA k. 85-87)

Powód miał dostęp do platformy bankowości elektronicznej niezmiennie od maja 2015 r. poprzez stronę internetową banku. Prawidłowość certyfikatu bezpieczeństwa jest weryfikowalna na podstawie ikony zamkniętej kłódki w pasu adresu strony internetowej. (...) S.A. W bankowości elektronicznej pozwany stosuje system dwustopniowej autoryzacji dostępu do konta. (...) bankowy przy logowaniu wymaga podania poprawnego numeru klienta i odpowiadającego mu hasła ustalanego przez klienta, a następnie przed ostatecznym zatwierdzeniem zlecenia płatności w trybie przelewu jednorazowego, podania kodu autoryzacyjnego z karty kodów jednorazowych wydawanej klientowi lub wysłanego klientowi wiadomością sms na wskazany numer telefonu kodu jednorazowego lub tokena generowanego w formie aplikacji lub specjalnego urządzenia. Wybór formy autoryzacji kodem należy do klienta, wszystkie formy są równie bezpieczne, o ile stosowane są zgodnie z procedurą bezpiecznego korzystania z bankowości elektronicznej. Klient może zdefiniować nowy szablon odbiorcy, wskazując jego numer rachunku oraz dane, przez co z góry autoryzuje zlecenia płatności na jego rzecz. Autoryzacja za pomocą kodów nie jest wymagana dla przelewów wewnętrznych między rachunkami tego samego klienta korzystającego z jednego numeru klienta w banku. Bank oferował klientom funkcję powiadomień sms o dokonywanych transakcjach. (dowód: okoliczności bezsporne, zeznania świadka J. K. k. 300-301, zeznania świadka J. G. k.301-301v zeznania P. C. k.301v-302).

(...) S.A. od kwietnia 2015 r. na stronie internetowej podaje komunikat o braku wymogu podawania kodu z narzędzia autoryzacyjnego podczas logowania na platformę bankowości elektronicznej. Komunikat pojawił się po atakach typu malware i phishing na klientów banku. (dowód: zeznania świadka J. G. k.301-301v)

Powód A. K. w maju 2015 roku korzystał z jednego konta klienta w systemie bankowości elektronicznej, w ramach którego obsługiwane były jego dwa rachunki bankowe – indywidualny i firmowy. Od 2014 roku autoryzacja dyspozycji dokonywanych przez pozwanego za pośrednictwem platformy bankowości elektronicznej z konta osobistego odbywała się poprzez kody sms wysyłane na numer telefonu (...). Powód nie miał ustanowionego alertu sms o dokonywanych na jego koncie transakcjach. Każdego dnia z rana otrzymywał wiadomość sms z banku z saldem konta. (dowód okoliczności bezsporne, zeznania J. K. k.300-301, zeznania powoda w charakterze strony k. 418-419).

Powód A. K. korzystając z bankowości elektronicznej w maju 2015 roku posługiwał się telefonem komórkowym marki A.(...) wyposażonym w zabezpieczenia uniemożliwiające dostęp do niego osobom nieuprawnionym oraz innym sprzętem komputerowym. Pozwany sprzedał komputer i tablet na których także korzystał z bankowości internetowej pozwanego w sierpniu 2015 roku. (dowód: okoliczności bezsporne, opinia biegłego k. 183-192, monitor logowań klientów (...)/ (...) k. 89-90, umowy sprzedaży k. 123-124, zeznania powoda w charakterze strony k. 418-419).

Na rachunkach bankowych przypisanych do A. K. w banku (...) S.A. odnotowywano miesięczny obrót sięgający kwoty ok. 8 mln zł, a dzienne dyspozycje przelewów przekraczały łączną kwotę 20.000 zł. W dniu 26 maja 2015 r. o godz. 12:23 oraz o godz. 12:25 A. K. autoryzował dwa przelewy z konta indywidualnego na kwoty po 16.644,84 zł. (dowód: opinia biegłego k. 183-192, zeznania powoda w charakterze strony k. 418-419).

W dniu 28 maja 2015 r. z rachunku bankowego A. K. o nr (...) w banku (...) S.A. nieustalony sprawca (sprawcy) złożyli dyspozycje przelewów natychmiastowych (...) w kwotach 19.570 zł, 17.000 zł, 19.800 zł, 19.915 zł, 19.100 zł, 24.000 zł, 18.000 zł (łącznie siedem przelewów na kwotę 137.285 zł) na rachunek bankowy o numerze (...) ze wskazaniem jako odbiorcy P. O.. Przelewy zostały dokonane podczas kilku logowań.

O godz. 10:11 nieznany sprawca zalogował się do systemu za pośrednictwem urządzenia o adresie IP (...) przynależnym do A. K. i złożył dyspozycję utworzenia nowego szablonu odbiorcy z konta A. K. na rzecz rachunku o numerze (...) z nazwą odbiorcy P. O.. A. K. o godz. 10:12 otrzymał wiadomość sms nr (...) z kodem do autoryzacji utworzenia nowego szablonu płatności, nie zwrócił na niego uwagi uznając, iż jest to sms ze saldem konta. Nie wykorzystał otrzymanego kody do autoryzacji odbiorcy zdefiniowanego. Nikomu nie udostępniał wiadomości sms w celu utworzenia odbiorcy zdefiniowanego, jednak kod został wykorzystany. (zestawienie wiadomości sms k. 245-248, monitor logowań klientów (...)/ (...) k. 89-90, raport z systemu retencji danych P4 sp zo.o. k. 389-390, zeznania powoda w charakterze strony k. 418-419).

Z tego samego adresu IP A. K. o godz. 10:35 zalogował się do systemu bankowości elektronicznej i złożył dyspozycję przelewu kwoty 18.900 zł na rachunek o numerze (...) tytułem „Zakup waluty symbol: (...)". Powód autoryzował transakcję wpisując kod SMS nr (...) otrzymany na wskazany numer telefonu. Podczas korzystania z platformy bankowości elektronicznej komputer A. K. nie pokazywał komunikatów o zainfekowaniu systemu wirusem. (dowód: szczegóły operacji (...) k. 227-228, zestawienie wiadomości sms k. 245-248, monitor logowań klientów (...)/ (...) k. 89-90, zeznania powoda w charakterze strony k. 418-419).

W okresie pomiędzy otrzymaniem pierwszej i drugiej wiadomości sms z banku zawierających kody autoryzacyjne, tj. o godz. 10:16, 10:19 i 10:22 A. K. wykonał trzy połączenia telefoniczne z wykorzystaniem numeru telefonu (...) co świadczy o tym, iż powód praktycznie nie rozstawał się telefonem (dowód: opinia biegłego k. 268-286).

O godz. 13:02:52 nieustalona osoba złożyła dyspozycję realizacji przelewu na kwotę 19.570 zł, zatytułowanego (...), na rzecz zdefiniowanego odbiorcy, za pośrednictwem urządzenia o adresie IP (...) (dowód: szczegóły operacji (...) k. 229-230, potwierdzenie przelewu k. 30, monitor logowań klientów (...)/ (...) k. 89-90).

Następnie z urządzenia posiadającego adres IP (...), w sesjach rozpoczętych kolejno o godz. 14:04:01, godz. 14:35:22 oraz godz. 14:35:22 złożono dyspozycje przelewów na kwoty 19.800 zł o tytule (...), 19.100 zł o tytule (...), 19.915 zł o tytule (...), 24.000 zł o tytule (...) oraz 18.000 zł o tytule (...). (dowód: szczegóły operacji (...) k. 231-232, szczegóły operacji (...) k. 233-234, szczegóły operacji (...) k. 235-236, szczegóły operacji (...) k. 237-238, szczegóły operacji (...) k. 239-240, potwierdzenia przelewów k. 32-36, monitor logowań klientów (...)/ (...) k. 89-90)

O godz. 14:38 (...) S.A. wysłał na numer telefonu komórkowego A. K. sms z kodem do autoryzacji przelewu na kwotę 19.915 zł na rachunek o numerze (...).. (...). Transakcja nie została zrealizowana wobec nieautoryzowania jej kodem. Zlecenie na tę kwotę ponowiono o godz. 14:39 i zostało zrealizowane na podstawie wcześniej zdefiniowanego szablonu odbiorcy (dowód: zestawienie wiadomości sms k. 245-248, załącznik do opinii k. 308-312).

Spod wskazanego adresu IP ((...)) logowano się do systemu również o godz. 15:10:36, podczas którego zrealizowano przelew między rachunkami A. K., tj. z rachunku o numerze (...) na rachunek o numerze (...) na kwotę 16.000 zł. Transakcję zrealizowano o godz. 15:26 bez użycia kodu autoryzacyjnego. (szczegóły operacji k. 241-242) Podczas tej sesji złożono również dyspozycję przelewu o tytule (...) na kwotę 17.000 zł na rachunek zdefiniowanego odbiorcy P. O.. (dowód: szczegóły operacji (...) k. 243-244, potwierdzenie przelewu k. 31, monitor logowań klientów (...)/ (...) k. 89-90).

(...) S.A. za dokonanie przelewów pobrał 7 opłat prowizyjnych po 40 zł. (dowód: potwierdzenia obciążenia rachunku opłatą k. 37-43)

Wszystkie środki finansowe z rachunku powoda zostały przekazane na rachunek zdefiniowanego odbiorcy P. O. w ciągu kilku minut od złożenia zleceń płatności w trybie przelewu natychmiastowego (...). (dowód: zeznania P. C. k. 301v-302).

Podczas logowań w dniu 28 maja 2015 r. do konta A. K. w bankowości elektronicznej (...) nie doszło do przełamania zabezpieczeń systemu bankowego, zaś procedura autoryzacji przelewów z rachunku powoda na nowo zdefiniowany rachunek odbiorcy P. O., została przeprowadzona w sposób zgodny z obowiązującymi w Banku procedurami. (dowód: opinia biegłego k. 268-286, zeznania świadka J. G. k. 301-301v, zeznania świadka P. C. k. 301v-302).

Wieczorem 28 maja 2015 roku, powód A. K., podczas codziennej weryfikacji stanu konta zorientował się o utracie środków pieniężnych z rachunków bankowych, po czym telefonicznie za pośrednictwem infolinii (...) S.A. oraz doradcy klienta indywidualnego J. K. złożył reklamację o nieautoryzowanych dyspozycjach z jego rachunku bankowego na łączną kwotę 137.285 zł. O godz. 21:25 złożył zawiadomienie o podejrzeniu popełnienia przestępstwa kradzieży w Komendzie Rejonowej Warszawa Policji VII. Reklamację ponowił osobiście udając się do oddziału banku w dniu 29 maja 2015 r. (dowód: okoliczności bezsporne, skarga k. 46, płyta CD k. 218, 430, protokół przyjęcia

zawiadomienia o podejrzeniu popełnienia przestępstwa k. 332-333v, zeznania świadka J. K. k. 300-301, zeznania świadka J. G. k. 301-301v, zeznania świadka P. C. k. 301v-302, zeznania powoda w charakterze strony k. 418-419).

Zawiadomienie o podejrzeniu popełnienia przestępstwa na szkodę A. K. złożył również bank (...) S.A. (dowód: okoliczność bezsporna).

Pismem z dnia 31 lipca 2015 r. (...) S.A. zawiadomił A. K. o nieuwzględnieniu reklamacji wskazując, że zlecenia płatności zostały złożone po poprawnym zalogowaniu w serwisie (...) numerem klienta oraz hasłem dostępu przynależnym do niego. Bank uznał, że klient logując się do konta korzystał ze zainfekowanej stacji roboczej. (dowód: pismo k. 114, zeznania świadka P. C. k. 301v-302).

W dniu 31 maja 2016 r. do Sądu Rejonowego Warszawa Praga Południe w Warszawie został skierowany akt oskarżenia przeciwko P. O., którym oskarżono go o to, że w okresie od dnia 11 maja 2015 r. do dnia 28 maja 2015 r. w W. działając wspólnie i w porozumieniu z innymi nieustalonymi osobami, w celu osiągniecia korzyści majątkowej, bez uprawnienia, po uprzednim przełamaniu elektronicznych zabezpieczeń prowadzonego przez bank (...) S.A. rachunku bankowego nr (...) na rzecz A. K. uzyskał nie przeznaczoną dla niego informację odnośnie stanu salda, a następnie zmienił zapis danych informatycznych w elektronicznym systemie bankowych w ten sposób, że z rachunku pokrzywdzonego A. K. dokonał niżej wymienionych transakcji-przelewów: kwoty 19.570 zł w dniu 28 maja 2015 r., kwoty 19.800 zł w dniu 28 maja 2015 r., kwoty 19.100 zł w dniu 28 maja 2015 r., kwoty 19.915 zł w dniu 28 maja 2015 r., kwoty 24.000 zł w dniu 28 maja 2015 r., kwoty 18.000 zł w dniu 28 maja 2015 r., kwoty 17.000 zł w dniu 28 maja 2015 r., tj. sumy 137.385 zł, którą to następnie kwotę przelał na założony przez siebie w dniu 11 maja 2015 r. w Oddziale Banku (...) w W. rachunek bankowy nr (...) na dane (...)C. P. O., po czym w dniu 28 maja 2015 r. dokonał wypłaty tych środków pieniężnych, działając tym na szkodę A. K. i Banku (...) S.A. z siedzibą w W., przy czym czynu tego dopuścił się w ciągu 5 lat po odbyciu co najmniej 6 miesięcy kary pozbawienia wolności za podobne przestępstwo umyślne, tj. o czyn z art. 278 § 1 kk w zw z art. 64 § 1 kk. (dowód: akt oskarżenia k. 412-415)

Powyższy stan faktyczny Sąd ustalił na podstawie okoliczności bezspornych, dowodów z dokumentów, których w ocenie Sądu były wiarygodne. Większość dokumentów, za wyjątkiem wydruków ze strony internetowej banku (k. 90-113) oraz wydruków z systemu informatycznego banku wskazujących na historię logowań do konta elektronicznego w bankowości elektronicznej powoda (k. 88-89), załączone do odpowiedzi na pozew, nie była kwestionowana przez strony, toteż Sąd nie znalazł podstaw by czynić to z urzędu. W ocenie Sądu jednak zakwestionowane dowody z dokumentów stanowiły pełnowartościową podstawę do poczynienia ustaleń faktycznych w sprawie, albowiem treść tych dokumentów była zgodna z wiarygodnymi zeznaniami świadków w części, w jakiej wskazywały na komunikaty banku o zasadach bezpiecznego logowania do systemu oraz opinią biegłego z zakresu informatyki i teleinformatyki (k. 268-286) oraz innymi wydrukami z systemu informatycznego banku (k. 227-244) w zakresie, w jakim wskazywały na logowania do systemu bankowości elektronicznej powoda. Złożone dokumenty posłużyły w szczególności do ustalenia szczegółów dotyczących logowania do konta powoda za pośrednictwem bankowości elektronicznej prowadzonej przez pozwany bank w spornym dniu, autoryzowania dokonania poszczególnych transakcji, podjętych przez bank działań informacyjnych względem klientów, w tym powoda, o zagrożeniach w korzystaniu z bankowości elektronicznej.

Sąd w szczególności uznał za przydatny i wiarygodny dowód z oględzin telefonu komórkowego sporządzony na wezwanie Sądu przez biegłego sądowego M. G. (k. 183-192) w części, w której biegły wskazywał na wyposażenie sprzętu w aktualne oprogramowanie oraz zabezpieczenia uniemożliwiające osobom trzecim dostęp do jego zawartości oraz aktualną wersję przeglądarki. Sąd pominął tę część dowodu, w której biegły wypowiadał się w sposób wykraczający poza granice właściwości dowodu z oględzin rzeczy.

Sąd uznał dowód z opinii biegłego sądowego M. G. za przydatny w zakresie w jakim biegły wskazywał na okoliczności zgodnie z zakreśloną tezą dowodową, rzeczowo odwołując się do faktów wynikających wprost z badań biegłego oraz zgromadzonego materiału dowodowego. Sąd oparł się na przedmiotowej opinii ustalając okoliczności dotyczące sprzętu, z jakiego nastąpiło logowanie do konta powoda w spornym dniu, wykluczenia możliwości zeskanowania karty sim powoda, częstotliwości korzystania przez powoda z telefonu komórkowego z przypisanym numerem

telefonu(...) w spornym dniu. Sąd pominął opinię w tej części, w jakim biegły wykraczał poza zakreślone granice tezy dowodowej, a w szczególności przedstawiał własne hipotezy co do zachowania powoda. Sąd mając przy tym na uwadze, że strony nie kwestionowały opinii, uznał, iż istnieją podstawy do poczynienia ustaleń faktycznych na jej podstawie we wskazanym powyżej zakresie. W ocenie Sadu opinia w tej części została sporządzona w sposób rzeczowy, rzetelny oraz przekonywujący w oparciu o wiedzę fachową, przez kompetentną osobę, posiadającą odpowiednie w tym kierunku specjalistyczne wykształcenie i wieloletnie doświadczenie zawodowe. Opinia jest jasna i logiczna, poparta przekonującymi wyjaśnieniami biegłego, z wyczerpującym uzasadnieniem i finalnie nie została zakwestionowana przez strony w tym w szczególności przez powoda, pomimo jednoznacznie niekorzystnych konkluzji z niej wynikających.

Pomocne dla poczynienia ustaleń faktycznych były również zeznania świadków J. K., J. G. i P. C., które Sąd ocenił jako wiarygodne. Świadkowie ci wskazali na stosowane przez bank środki powiadomienia klientów o zagrożeniach związanych z korzystaniem z bankowości elektronicznej, metodach weryfikacji bezpieczeństwa użytkowania platformy, jak również przebiegu procesu reklamacji oraz realnych przyczyn odmowy jej uwzględnienia. Zeznania świadków były spójne, logicznie i w sposób wzajemnie się uzupełniający. Zeznania te korespondowały ze zgromadzonymi w sprawie dowodami z dokumentów, a w szczególności z opinią biegłego z zakresu informatyki i teleinformatyki.

Za wiarygodne Sąd uznał zeznania powoda w charakterze strony w części, w której podawał na okoliczność otrzymania i odczytania wiadomości sms od pozwanego banku z kodami do autoryzacji utworzenia nowego szablonu płatności i przelewu na kwotę 19.915 z; oraz korzystania podczas obsługi bankowości elektronicznej ze sprzętu, co do którego nie miał wiedzy o stanie zabezpieczeń. Powód wiarygodnie nadto opisał szczegóły zawiadomienia odpowiednich osób o utracie środków pieniężnych z rachunku bankowego oraz braku znajomości z P. O..

Sąd Okręgowy zważył, co następuje:

Powództwo jako bezzasadne podlegało oddaleniu w całości.

Na wstępie wskazać należy, iż bezsporny między stronami był fakt zawarcia umowy usług bankowości elektronicznej oraz rachunku oszczędnościowo-rozliczeniowego, jak również, iż w dniu 28 maja 2015 r. nieustalony użytkownik niezwiązany ze stronami złożył pozwanemu dyspozycję utworzenia zdefiniowanego odbiorcy na koncie przypisanym indywidualnie do powoda, a następnie złożył 8 zleceń płatniczych – przelewów natychmiastowych typu (...), w tym jedno bezskuteczne, na rachunek bankowy o numerze (...), przynależny do P. O., na łączną kwotę 137.285 zł. Poza sporem był fakt, iż powód w dniu 28 maja 2015 r. ok. godz. 10:12 otrzymał, a następie odczytał z banku wiadomość sms zawierającą kod autoryzacyjny do utworzenia w/w zdefiniowanego odbiorcy, jak również ok. godz. 14:38 wiadomość sms o dyspozycji przelewu na ww rachunek kwoty 19.915 zł. Sporna natomiast między stronami okoliczność autoryzacji dyspozycji utworzenia nowego zdefiniowanego odbiorcy, zwolnienia banku z obowiązku uzyskania zgody użytkownika na dokonanie kolejnych transakcji, przełamania zabezpieczeń powoda i pozwanego w związku z wysłaniem płatnikowi instrumentu płatniczego oraz obciążającego bank ryzyka w związku z tym.

W niniejszej sprawie podstawy odpowiedzialności wynikające z wykonania zawartej między stronami postępowania umowy rachunku oszczędnościowo-rozliczeniowego Konto P. (...), usług bankowości elektronicznej oraz karty debetowej bez (...) z dnia 20 czerwca 2011 r. regulują przepisy ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (dalej: uup), które wyznaczają minimalny standard praw i obowiązków stron umowy o usługę płatniczą.

Zgodnie z art. 42 uup użytkownik, w niniejszej sprawie powód, korzystając z instrumentu płatniczego zobowiązany jest do korzystania z instrumentu płatniczego zgodnie z umową ramową (ust. 1 pkt 1) poprzez podejmowanie niezbędnych środków służących zapobieżeniu naruszenia indywidualnych zabezpieczeń tego instrumentu, w szczególności do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go innym osobom (ust. 2) oraz do zgłaszania niezwłocznego dostawcy – w niniejszej sprawie pozwanemu bankowi, lub

podmiotowy wskazanemu przez dostawcę stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego do tego instrumentu (ust. 1 pkt 2).

Dostawca zaś zobowiązany jest m. in. zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu (art. 43 ust. 1 pkt 1 uup) oraz uniemożliwienia korzystania z instrumentu płatniczego po dokonaniu zgłoszenia zgodnie z art. 42 ust. 1 pkt 2 (art. 43 ust. 1 pkt 5 uup). Na mocy art. 43 ust. 2 uup dostawcę obciąża ryzyko związane z wysłaniem płatnikowi instrumentu płatniczego lub jego indywidualnych zabezpieczeń.

Dostawca jest zobowiązany do niezwłocznego zwrotu płatnikowi kwoty nieautoryzowanej transakcji płatniczej, o ile transakcja była nieautoryzowana i jest skutkiem: 1) posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub 2) przywłaszczenia instrumentu płatniczego lub jego nieuprawnionego użycia w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2. (art. 46 ust. 1 uup).

Ustawodawca w art. 46 ust. 3 uup wskazuje natomiast, że płatnik 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/w ustawy.

Zgodnie z art. 50 § 2 prawa bankowego bank dokłada szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Przepis art. 50 ust 2 ustawy z dnia 29 sierpnia 1997 r. prawa bankowego i art. 355 § 2 kc mają charakter norm imperatywnych, bezwzględnie obowiązujących. Stworzone zostały przez ustawodawcę w celu wspierania i ochrony strony słabszej, jaką wobec profesjonalisty, którym jest bank, pozostaje jego kontrahent - posiadacz rachunku bankowego. Od banku wymaga się bowiem należytej staranności w wykonaniu zobowiązania wynikającego z zawieranych z klientami banku umów prowadzenia rachunku.

W ocenie Sądu pozwany prawidłowo wywiązał się z nałożonych na niego obowiązku nieudostępniania innym osobom niż powód zabezpieczeń instrumentu płatniczego. Z opinii biegłego z zakresu informatyki i teleinformatyki jak również z zeznań świadków – pracowników pozwanego banku wynika, iż nie doszło do przełamania żadnych zabezpieczeń banku. Logowania do konta powoda w systemie bankowości elektronicznej odbywało się z wykorzystaniem jego osobistego numeru klienta oraz ustanowionego przez niego hasła. (...) bankowy odczytywał próby logowania na konto jako działanie uprawnionego użytkownika – powoda. Powód zaś mimo realnej możliwości niemalże natychmiastowego zgłoszenia bezprawnych działań skierowanych wobec przynależnych do niego rachunków bankowych, nie wykazał dbałości o własne życiowe sprawy i dopiero wieczorem złożył reklamację. Powód, reprezentowany przez profesjonalnego pełnomocnika, nie wykazywał inicjatywy dowodowej zmierzającej do obalenia twierdzeń świadków, nie kwestionował również opinii biegłego w tym zakresie. Nie zgłaszał również wniosków dowodowych zmierzających do wykazania niepoprawności działania systemu bankowego.

W toku całego procesu nie doszło do wykazania przez powoda zgodnie z obciążającym go ciężarem dowodu, iż można przypisać pozwanemu działania umyślne lub będące skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków o których mowa w art.42 ustawy o usługach płatniczych (art.46 ust.3 ustawy o usługach płatniczych).

W ocenie Sądu nie można także przypisać pozwanemu odpowiedzialności na takiej podstawie, iż nie doszło do automatycznego zablokowania dostępu do instrumentu płatniczego po autoryzacji utworzenia zdefiniowanego odbiorcy, skorzystaniu z funkcji przelewu natychmiastowego (...), a następnie również po wykonaniu pierwszych dwóch transakcji, których ogólna wartość przekroczyła kwotę 20.000 zł. Fakt, iż powód wcześniej nie korzystał z funkcji zdefiniowanego odbiorcy oraz przelewów natychmiastowych, nie może stanowić podstawy dla systemu, w razie z niej skorzystania, że dostęp do instrumentu płatniczego uzyskała osoba nieuprawniona. Nie można bowiem oczekiwać od pozwanego, że wykorzystanie przez klienta nowo wprowadzonych funkcjonalności takich jak możliwość tworzenia zdefiniowanych odbiorców czy przelewy (...) będzie jednocześnie podstawą do zablokowania dostępu do systemu bankowości elektronicznej. Bank nie narzuca bowiem klientom obowiązku korzystania ze wszystkich narzędzi systemowych, pozostawia mu swobodę decydowania z jakich rozwiązań korzysta. Odnosząc się zaś do przekroczenia progu 20.000 zł w dwóch transakcjach, zdaniem Sądu, złożenie zleceń przelewów na kwoty przewyższające wskazany

próg nie stanowiło nietypowego działania w ramach konta powoda w bankowości elektronicznej. Sam powód przyznał, iż miesięcznie obracał na swoich rachunkach kwotami kilkumilionowymi, biegły z zakresu informatyki i teleinformatyki odczytał zaś, że np. powód na dwa dni przed utratą środków finansowych w ciągu dwóch minut złożył autoryzowane zlecenia przelewów na łączną kwotę 33.289,68 zł. co dawało systemowi bankowemu informację o nietypowych zachowaniach powoda w zakresie korzystania ze zgromadzonych środków finansowych.

Wyniki postępowania dowodowego pozwoliły na stwierdzenie, iż to powód nie wywiązał się z obowiązku wskazanego w art. 42 ust. 2 uup nieudostępniania instrumentu płatniczego osobom nieuprawnionym oraz nie podjął niezbędnych kroków mających na celu naruszenie indywidualnych zabezpieczeń urządzeń elektronicznych z których logował się do systemu bankowego pozwanego. Znamienny jest fakt, iż praktycznie 2 miesiące po utracie środków finansowych z konta powoda, powód sprzedał urządzenia elektroniczne z których m.in. korzystał z bankowości internetowej pozwanego (umowa sprzedaży z dnia 31.08.2015 roku k. 123, i 26.08.2015 k. 124), co uniemożliwiło weryfikację twierdzeń powoda w zakresie korzystania przez niego ze sprzętu rekomendowanego przez pozwanego, z aktualnym oprogramowaniem antywirusowym. Dla odpowiedzialności karnej sprawców którzy wyprowadzili środki finansowe z konta powoda ta okoliczność może pozostawać bez znaczenia albowiem doszło do przywłaszczenia środków finansowych wbrew woli powoda, jednakże dla odpowiedzialności cywilnej pozwanego ma to istotne znaczenie, z uwagi na wykazanie należytej staranności ze strony powoda w zakresie podjęcia niezbędnych środków służących zapobieżeniu naruszeniu indywidualnych zabezpieczeń oraz nieudostępnienia dostępu do konta osobom postronnym.

Trudno w ocenie Sądu obciążać odpowiedzialnością pozwanego za dokonane nieautoryzowane przez powoda transakcje, w sytuacji gdy cała procedura autoryzacji przelewów w dniu 28 maja 2015 roku została przeprowadzona w sposób zgodny z obowiązującymi procedurami. Pozwany Bank mając na względzie bezpieczeństwo zgromadzonych środków finansowych, wydał zalecenia zarówno w zakresie stosowania sprzętu, oprogramowania jak również sposobu postępowania w zakresie bezpiecznego korzystania z bankowości elektronicznej. Także dwustopniowa procedura autoryzacji zleceń dodatkowo to bezpieczeństwo ma poprawiać. Nie można jednak wymagać od Banku i obciążać go odpowiedzialnością za własne niedbalstwo, oraz niedochowanie należytej staranności w zakresie zabezpieczeń sprzętu elektronicznego z którego użytkownik dokonuje transakcji w systemie bankowości elektronicznej.

Jak bowiem wynika z materiału dowodowego, logowanie do konta powoda w bankowości elektronicznej nastąpiło z IP z którego korzystał powód. Biegły sądowy z zakresu informatyki i teleinformatyki odczytał spójnie z zestawieniami sporządzonymi przez pozwany bank, iż logowanie do systemu podczas, którego utworzony nowy szablon płatności zdefiniowanego odbiorcy nastąpiło z tego samego IP, z którego po 26 minutach zalogował się powód by dać zlecenie płatnicze zakupu waluty. Nadto powód w czasie, w którym nastąpiła autoryzacja utworzenia zdefiniowanego odbiorcy w ramach udostępnianego mu instrumentu płatniczego korzystał z telefonu komórkowego, do którego przypisany był numer telefonu, pod który pozwany bank kierował wiadomości sms z kodami autoryzacyjnymi. Powód nie kwestionował tej okoliczności. W toku procesu nie ustalono w jaki konkretnie sposób nieuprawnione przez powoda osoby lub osoba uzyskały informację o numerze klienta, haśle oraz kodzie autoryzacyjnym, jednak nie można w tym zakresie jakiekolwiek winy przypisać pozwanemu banku. Wskazać jednak należy, że czynności te zostały odczytane przez zautomatyzowany system bankowy jako czynności uprawnionego użytkownika. Zlecenie zostało złożone po pozytywnym przejściu systemu dwustopniowej autoryzacji.

W ocenie Sądu pozwany bank wykazał, że powód jako użytkownik autoryzował utworzenie nowego szablonu płatności, która to zgoda, stosownie do art. 40 ust. 1 uup odnosiła skutek do kolejnych transakcji płatniczych na rzecz tego odbiory. Stosownie do art. 45 ust. 1 i 2 upp ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika i polega na udowodnieniu innych niż wskazanie zarejestrowanego użycia instrumentu płatniczego okoliczności wskazujących 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/w ustawy.

Należy zauważyć, że pozwany przyznał, iż w obsłudze instrumentu płatniczego posługiwał się kilkoma urządzeniami komputerowymi, w tym tabletem i laptopem, które po utracie środków finansowych z rachunku poddał badaniu pod kątem zawirusowania, a następnie zbył w obawie przed ponownymi atakami. Logowania do systemu poprzez inny sprzęt niż telefon komórkowy marki A.(...)zostały potwierdzone wydrukami z systemu informatycznego banku oraz opinią biegłego z zakresu informatyki i teleinfomartyki. W ocenie Sądu powodowi można przypisać co najmniej nieumyślne doprowadzenie do autoryzowania transakcji płatniczych, albowiem posługiwał się on komputerem co do którego nie miał pewności o wyposażeniu w aktualne oprogramowanie antywirusowe, antyspamowe i zaporę firewall. Powód nadto przechowywał ten komputer w pracy, a więc w miejscu, gdzie teoretycznie dostęp do niego miała nieograniczona liczba osób o tożsamości niemożliwej do zidentyfikowania. Tymczasem pozwany bank w regulaminie korzystania z bankowości elektronicznej jasno określał użytkownikom wymagania dotyczących oprogramowania. Nadto bank na stronie internetowej umożliwiającej logowanie do systemu udostępniał użytkownikom kompendium wiedzy o bezpiecznym logowaniu do systemu, a w szczególności o metodach weryfikowania, czy logowanie odbywa się za pośrednictwem oryginalnej strony internetowej pozwanego banku. Powód logując się do systemu miał możliwość zapoznania się z choćby pojawiającymi się komunikatami o zagrożeniach w sieci ukierunkowanych na klientów bankowości elektronicznej. Komunikaty bowiem zostały ujawnione na stronie internetowej banku co najmniej na miesiąc przed spornym dniem, a powód każdego dnia sprawdzał salda rachunków za pośrednictwem systemu informatycznego. Zaniedbanie przez powoda zasad bezpieczeństwa stanowiło ułatwienie dla hakerów do włamania się do komputera czy tableta powoda i skopiowanie z tego sprzętu danych umożliwiających dostęp do konta w bankowości elektronicznej powoda.

W takim stanie rzeczy Sąd uznał, że nie ma podstaw do uznania, że pozwany bank uchybił swoim obowiązkom wynikającym z art. 46 ust. 1 uup. W aktualnym stanie prawnym brak jest podstaw do uznania, iż dostawca instrumentu – bank, będący profesjonalistą w obrocie gospodarczym zobowiązany jest do zapewnienia zabezpieczeń indywidualnych dla systemów komputerowych płatników, a także do analizy prawdziwości danych wychodzących z komputerów użytkowników pod kątem, czy nie stanowią one wyniku działania przestępczego. Korzystanie z usług płatniczych w świetle obecnie obowiązującej ustawy opiera się na umowie stron i ich współdziałaniu w bezpiecznym korzystaniu z dobrodziejstwa postępu technologicznego umożliwiającego obrót bezgotówkowy. Z uwagi na fakt, iż regulamin świadczenie usług bankowości elektronicznej (...) powielał przepisy ustawy o prawach i obowiązkach stron dotyczących korzystania z instrumentu płatniczego, w tym zasadach autoryzacji zleceń płatniczych, to nie ma również podstaw do uznania odpowiedzialności kontraktowej pozwanego banku (art.471 k.c.). Zgromadzony materiał dowodowy nie stwarza warunków do uznania, iż pozwany banku dopuścił jakichkolwiek uchybień przy zabezpieczeniu instrumentu płatniczego przypisanego powodowi przed dostępem dla nieuprawnionych użytkowników lub w inny sposób nienależycie wykonywał swoje zobowiązanie.

Gdyby nawet poszukiwać odpowiedzialności pozwanego ex delicto (art.415 k.c.) w ocenie Sądu również w tym zakresie nie można uznać, iż powód wykazał wszystkie przesłanki odpowiedzialności odszkodowawczej. Pomimo niewątpliwie istniejącej szkody jaką poniósł powód, nie została wykazana najmniejsza wina pozwanego związana z naruszeniem obowiązujących norm, czy też wynikająca z niesprawności systemów bankowych pozwanego, a wręcz przeciwnie biegły w swojej opinii wprost wskazywał, iż nie doszło do przełamania zabezpieczeń systemu bankowego pozwanego, zaś cała procedura autoryzacji przelewów została przeprowadzona zgodnie z wewnętrznymi procedurami Banku.

Mając na uwadze fakt, iż to powód uchybił wykonaniu obowiązku podjęcia niezbędnych środków służących zapobieżeniu naruszenia indywidualnych zabezpieczeń dostępu i używania konta w systemie bankowości elektronicznej, określonego w art. 42 ust. 2 uup, to on ponosi odpowiedzialność za nieautoryzowane przelewy z jego konta na obcy rachunek bankowy (art. 46 ust. 3 uup).

Z uwagi na powyższe Sąd oddalił powództwo w całości (pkt.1 wyroku).

Konsekwencją powyższego było orzeczenie o kosztach sądowych, które Sąd oparł o art. 98 kpc, normującego odpowiedzialność za wynik procesu, zgodnie z którym strona przegrywająca sprawę obowiązana jest zwrócić przeciwnikowi na jego żądanie koszty niezbędne do celowego dochodzenia praw i celowej obrony (koszty procesu).

Sąd obciążając powoda obowiązkiem zwrotu kosztów procesu uznał, że złożyły się na nie: poniesione przez pozwanego koszty opinii biegłego w kwocie 991,07 zł, opłata skarbowa od pełnomocnictwa w kwocie 17 zł, koszty zastępstwa procesowego udzielonego pozwanemu przez adwokata w kwocie 3600 zł, ustalonej na podstawie § 6 pkt 6 Rozporządzenia Ministra Sprawiedliwości z dnia 28.09.2002 roku w sprawie opłat za czynności adwokackie..., które ma zastosowanie do spraw wszczętych i zakończonych w instancji przed dniem 1 stycznia 2016 rok (pkt. 2 wyroku).

Na podstawie art. 113 ust.1 ustawy o kosztach sądowych w sprawach cywilnych w zw. z art.98 kpc, Sąd nadto obciążył powoda obowiązkiem uiszczenia kosztów opinii biegłego w kwocie 1.422,67, które zostały tymczasowo pokryte przez Skarb Państwa (k.197), o czym orzekł w pkt 3 wyroku.

Mając powyższe na względzie, Sąd orzekł jak w wyroku.---

/-/ SSO Mariusz Solka

ZARZĄDZENIE

1. (...)

2. (...)

3. (...)

(...)