Sygnatura akt I C 1206/14

# WYROK
## W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

(...), dnia 24 listopada 2015 r.

***Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi I Wydział Cywilny*** w następującym składzie:

Przewodniczący: SSR Katarzyna Barańska

Protokolant: starszy sekretarz Iwona Kamińska

po rozpoznaniu w dniu 29 października 2015 r. w Łodzi

na rozprawie

sprawy z powództwa T. P. (1)

przeciwko (...) SA w W.

- o zapłatę

1. zasądza od (...) Spółki Akcyjnej z siedzibą w W. na rzecz T. P. (1) kwotę 24.296,40 zł (dwadzieścia cztery tysiące dwieście dziewięćdziesiąt sześć złotych czterdzieści groszy) z ustawowymi odsetkami od dnia 31 października 2014 roku do dnia zapłaty;

2. oddala powództwo w pozostałej części;

3. zasądza od (...) Spółki Akcyjnej z siedzibą w W. na rzecz T. P. (1) kwotę 3.632 zł (trzy tysiące sześćset trzydzieści dwa złote) tytułem zwrotu kosztów procesu.

Sygn. akt I C 1206/14

# UZASADNIENIE

Pozwem z dnia 10 października 2014 r. skierowanym przeciwko (...) S.A. w W. powód T. P. (1) wniósł zasądzenie od pozwanego na jego rzecz kwoty 24.296,40 zł wraz z ustawowymi odsetkami liczonymi od dnia 22 stycznia 2014 r. do dnia zapłaty oraz kosztami postępowania, w tym kosztami zastępstwa radcowskiego według norm przepisanych. (pozew k. 2 – 7)

Nakazem zapłaty z dnia 24 października 2014 r. Sąd orzekł zgodnie z żądaniem powoda. (nakaz zapłaty k. 59)

W sprzeciwie od nakazu zapłaty pozwany wniósł oddalenie powództwa. Podniósł zarzut przyczynienia się poszkodowanego do powstania szkody w 50% (sprzeciw k. 62 – 65)

Strony do końca procesu podtrzymały swoje stanowiska w sprawie.

Pełnomocnik powoda wniósł o nieobciążanie powoda kosztami procesu w przypadku oddalenia powództwa (k. 251)

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

W dniu 4 listopada 2010 r. powód T. P. (1) zawarł z (...) oddziałem pozwanego (wówczas działającym pod nazwą (...) Bank Spółka Akcyjna z siedzibą w W., (...) Banku S.A. (...)-(...) Ł., Al. (...)) umowę o świadczenie usług bankowych w

MultiBanku, na podstawie której otwarte zostało (...) o numerze (...) w powiązaniu z rachunkiem oszczędnościowym (...) nr rachunku (...). Na podstawie tej umowy otwarty został również rachunek bankowy (...) nr rachunku (...).

Zgodnie z § 7 pkt 1 umowy o świadczenie usług bankowych w MultiBanku w zakresie nieuregulowanym zapisami Umowy, Umów rachunków i Umów kredytów zawartych na jej podstawie, stosuje się m. in. „Regulamin otwierania i prowadzenia rachunków bankowych dla osób fizycznych w MultiBanku.

§34 powołanego Regulaminu stanowi:

1. Autoryzacja transakcji płatniczych przez Płatnika oraz potwierdzenie złożenia dyspozycji przez Posiadacza Rachunku może nastąpić poprzez;

1) złożenie przez Posiadacza Rachunku podpisu zgodnego z Kartą Wzoru Podpisu lub z podpisem złożonym na Umowie - w przypadku dyspozycji, w tym zleceń płatniczych składanych w formie pisemnej lub w placówce Banku;

2) wprowadzenie hasła jednorazowego- w przypadku dyspozycji, w tym zleceń płatniczych składanych w kanałach dostępu o których mowa w §27 ust.l pkt. 1-2;

3) nagraną i utrwaloną przez Bank dyspozycję Posiadacza Rachunku - w przypadku dyspozycji, w tym zleceń płatniczych składanych w kanale dostępu o którym mowa w §27 ust.l pkt. 2.

2. Z chwilą wykonania czynności wskazanych w ust.l zlecenie płatnicze lub dyspozycję uznaje się za otrzymaną przez Bank i nie może być odwołane, z zastrzeżeniem §52 oraz o ile dokumenty stanowiące integralną część Umowy nie stanowią inaczej.

3. Autoryzacja transakcji płatniczej przez Płatnika, która została wykonana przy pomocy prawidłowego identyfikatora i hasła w sposób wskazany w ust. l nie może zostać wycofana przez Płatnika po jej otrzymaniu przez Bank.

4. Potwierdzenie złożenia dyspozycji przez Posiadacza Rachunku, które zostało wykonane przy pomocy prawidłowego identyfikatora i hasła w sposób wskazany w ust. l nie może zostać wycofane przez Posiadacza Rachunku po jego otrzymaniu przez Bank.

5. Posiadacz Rachunku zobowiązany jest upewnić się, że wszystkie składane przez niego dyspozycje, w tym zlecenia płatnicze są prawidłowe i zgodne z jego intencją. Ponadto Posiadacz Rachunku powinien osobiście i skutecznie wylogować się z danego kanału dostępu (np. przerwać połączenie telefoniczne) po złożeniu przez niego dyspozycji, w tym zlecenia płatniczego w sposób zapewniający bezpośredni osobisty nadzór danego kanału dostępu.

6. O przypadkach nieautoryzowanych lub nieprawidłowo wykonanych transakcji płatniczych, Płatnik lub Odbiorca informuje Bank za pośrednictwem BOK lub placówki Banku w terminie 7 dni od dnia otrzymania informacji od Banku lub uzyskania tej informacji w inny sposób w zależności od tego, które z tych okoliczności zaistniało jako pierwsze. O ile roszczenia Płatnika względem Banku nie wygasły zgodnie z (...), w przypadku wystąpienia nieautoryzowanej transakcji płatniczej Bank jest obowiązany niezwłocznie zwrócić Płatnikowi kwotę nieautoryzowanej transakcji płatniczej poprzez przywrócenie obciążonego Rachunku do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

7. 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, jeżeli nieautoryzowana transakcja jest skutkiem:

8. posłużenia się utraconą przez Płatnika albo skradzioną Płatnikowi debetową kartą płatniczą, bądź innym instrumentem płatniczym w rozumieniu (...), lub

9. przywłaszczenia debetowej karty płatniczej bądź innego instrumentu płatniczego w rozumieniu (...) lub ich nieuprawnionego użycia w wyniku naruszenia przez Płatnika obowiązków określonych w niniejszym Regulaminie lub Regulaminie wydawania i używania debetowych kart płatniczych w MultiBanku.

10. 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 którym mowa w Dziale II Rozdziale VI niniejszego Regulaminu.

11. Po dokonaniu przez Płatnika niezwłocznego zgłoszenia stwierdzenia utraty, kradzieży, przywłaszczenia debetowej karty płatniczej bądź innego instrumentu płatniczego w rozumieniu (...) albo nieuprawnionego ich użycia lub nieuprawnionego do nich dostępu Płatnik nie odpowiada za nieautoryzowane transakcje płatnicze, chyba że Płatnik doprowadził umyślnie do nieautoryzowanej transakcji płatniczej.

12. Jeżeli Bank, wbrew obowiązkowi zapewnienia stałej dostępności odpowiednich środków pozwalających Płatnikowi na dokonanie zgłoszenia o którym mowa w ust. 9, lub wystąpienia z wnioskiem o odblokowanie Rachunku, nie zapewnia takich możliwości, Płatnik nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że Płatnik doprowadził umyślnie do nieautoryzowanej transakcji płatniczej

§41 Regulaminu stanowi:

1. Posiadacz Rachunku jest zobowiązany do należytego zabezpieczenia narzędzi i urządzeń, z których korzysta w celu uzyskania dostępu do Rachunku, w szczególności poprzez:

1) nie omijanie fabrycznych zabezpieczeń urządzeń telekomunikacyjnych;

2) zainstalowanie na urządzeniu legalnego oprogramowania systemowego oraz antywirusowego;

3) pobranie aplikacji mobilnej w sposób wskazany przez Bank:

a) za pośrednictwem strony internetowej Banku;

b) za pośrednictwem BOK.

4) dokonywanie aktualizacji zainstalowanego na urządzeniu legalnego oprogramowania systemowego oraz antywirusowego.

2. Niezachowanie przez Posiadacza Rachunku należytej staranności w zakresie o którym mowa w ust. l jest jednoznaczne z wyłączeniem odpowiedzialności Banku z tytułu szkód wynikających z postępowania Posiadacza Rachunku w sposób sprzeczny z postanowieniami ust. l, które wystąpiły z powodu okoliczności niezawinionych przez Bank.

(umowa z dnia 4 listopada 2010 r. o świadczenie usług bankowych k. 41 – 44, regulamin k. 67 - 82)

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. 11 – 40)

W dniu 21 stycznia 2014 r. ok. godz. 13.45 - 14.20 powód zalogował się do konta za pośrednictwem systemu bankowości elektronicznej pozwanego. Dokonał transakcji przelewu na kwotę 700 zł na rzecz A. C. i tę transakcję potwierdził sms - em. Przed wykonaniem przelewu powód sprawdził, czy jest na prawidłowej stronie banku. Następnie podczas próby zasilenia telefonu córki przy użyciu systemu płatności „wyrzuciło" go ze strony banku. Zalogował się ponownie, przeszedł do zakładki celem zapłacenia za telefon P. i ponownie wrzuciło go ze strony. Powód nadal próbował zalogować się. Pojawił się komunikat, że jest w strefie zagrożonej i jego system komputerowy zaczął migać żółtą

zakładką „jesteś w strefie zagrożonej zabierz mnie stąd". Powód nie wykonał więc w tym dniu już żadnej transakcji, a o zaistniałej sytuacji zawiadomił telefonicznie na numer (...) A. J. (1) – pracownicę pozwanego zajmującą się obsługą kont M. A. w placówce pozwanego banku znajdującej się w G. przy ul. (...). A. J. poprosiła standardowo, aby klient wylogował się i zalogował jeszcze raz a jeśli kłopot będzie się powtarzał, to ma się zgłosić ponownie i wówczas powiadomi departament (...) Banku. Po przytoczonej wyżej rozmowie A. J. (1) uznała, że powód ma problem z komputerem skoro „wyrzuca" go ze strony banku i nie zgłosiła tego faktu do departamentu bezpieczeństwa. W międzyczasie A. J. (1) zakończyła pracę. A. J. (1) nie przekazała koleżance informacji, że jeżeli powód poinformuje, że kłopoty się powtarzają, to należy zawiadomić departament bezpieczeństwa. T. P. (1) podjął dwukrotną próbę i dwukrotnie wyrzuciło go ze strony po wejściu w zakładkę (...). Ponieważ musiał już opuścić dom, zadzwonił do A. J. (1) z samochodu i nagrał wiadomość, którą to wiadomość odebrała rano następnego dnia. (zeznania świadka A. J. (1) k. 191 – 192, zeznania powoda k. 187 – 190 w zw. z k. 252)

W dniu 21 stycznia 2014 r. niezidentyfikowany sprawca dokonał bez wiedzy i zgody powoda szeregu operacji na ww. rachunkach bankowych. Z rachunku M. A. przelał na M. A. kwotę 24.390 zł. Następnie tego samego dnia, ok. godz. 16:42 nieznany sprawca bez wiedzy i zgody powoda wyprowadził z rachunku powoda M. A. kwotę 24.296,40 zł na zewnętrzny rachunek bankowy zarejestrowany na nieznaną powodowi osobę oznaczoną jako J. P., prowadzony w pozwanym banku o numerze: (...). W tytule przelewu wskazano: (...). (okoliczności bezsporne)

Około godziny 22.00 tego samego dnia powód zalogował się do systemu bankowości elektronicznej pozwanego i spostrzegł w historii rachunku ww. przelew wewnętrzny z subkonta M. A. na rachunek główny M. A. na kwotę 24 390,00 zł oraz przelew zewnętrzny wychodzący na kwotę 24.296,40 zł na rzecz nieznanej powodowi osoby (...). Powód miał wrażenie, że pieniędzy na jego koncie było więcej. Stwierdził w historii rachunku brak zasileń (uznań) konta. Miał wrażenie, że niezidentyfikowana osoba oprócz wyprowadzenia kwot, ingerowała również w historię operacji i saldo rachunku. W celu wykonania przelewu trzeba wprowadzić nowego odbiorcę, zaś powód nie wprowadzał odbiorcy (...) + J. P. i nie zatwierdzał tej transakcji sms'em. T. P. (1) nie potwierdzał ustanowienia odbiorcy zaufanego J. P.. Przelewy własne z konta oszczędnościowego na rachunek bieżący wymagały dodatkowego potwierdzenia hasłem z sms-a. W tym dniu powód nie potwierdzał takich przelewów i nie widział sms-ów z takimi hasłami. Takie sms-y nie przyszły również, gdy był przy komputerze. Powód ma telefon starego typu z niewielką pamięcią i sms-y musi kasować na bieżąco. Nie wpisywał nigdzie hasła, aby potwierdzić transakcję (zeznania powoda k. 187 – 190 w zw. z k. 252, nagrania rozmów telefonicznych nagrania rozmów telefonicznych z dnia 21 stycznia 2014 r., z dnia 22 stycznia 2014 r., płyta k. 94).

Aby doszło do zainstalowania na telefonie programu szpiegowskiego musi być telefon z systemem android, windows lub innym podobnym i dostępem do Internetu. Na starych telefonach nawet mających dostęp do Internetu nie było możliwości zainstalowania takiego programu. (zeznania świadka M. W. k. 228 - 232)

Około 23:00 powód poinformował o tym zdarzeniu pozwany bank za pośrednictwem systemu telefonicznego pozwanego banku z nr (...), zgłaszając reklamację T. P. (2). Rozmowa została nagrana przez system bankowej rejestracji. Reklamacja została zarejestrowana pod numerem (...). Pracownik stwierdził na historii rachunku klienta przelew wewnętrzny na inne konto w mBanku, którego powód nie autoryzował. Następnie zablokował kanał internetowy, dostęp sms – owy, założył blokadę na obciążenia, zalecił zmianę trybu autoryzacji. Pracownik banku nie dokonał blokady rachunku, z braku takich uprawnień. Dyspozycję tę przyjął i miał przekazać do departamentu bezpieczeństwa, który działał od godziny 7:00 do 17:00. Pracownicy tego departamentu mieli się zgłosić do powoda rano następnego dnia. Godzinę później powód ponownie skontaktował się z pozwanym za pośrednictwem systemu telefonicznego pozwanego - rozmowa została nagrana przez system bankowej rejestracji. Podczas drugiej rozmowy powód zaproponował, aby zablokować konto J. P. - osobie na której konto „poszedł" przelew. Rozmówca – pracownik pozwanego banku (...) oświadczył, że nie ma takiej możliwości, jako pracownik infolinii, ma ją tylko departament bezpieczeństwa, któremu reklamacja została przypisana. Ponownie potwierdzono, że blokady rachunku powoda może dokonać wyłącznie departament bezpieczeństwa. Przeanalizowano wówczas historię obciążeń na rachunku powoda oraz powód poprosił o informację o dane firmy (...), na który został dokonany przelew z konta powoda. Powoda poinformowano, że mBanku ma ubezpieczenie w Bankowym Funduszu Gwarancyjnym. Trzecia rozmowa również

nie spowodowała zasadniczego zwrotu w sprawie. (zeznania powoda k. 187 – 190 w zw. z k. 252, nagrania rozmów telefonicznych nagrania rozmów telefonicznych z dnia 21 stycznia 2014 r., z dnia 22 stycznia 2014 r., płyta k. 94***)***

Konto powoda zablokowane zostało w dniu 22. 01.2014 r. przez pracownika Departament (...) Banku (zeznania świadka M. W. k. 228 - 232)

Rano 22 stycznia 2014 r. po odsłuchaniu wiadomości od powoda A. J. (1) sprawdziła jego rachunek i stwierdziła, że informacje powoda o wyprowadzeniu środków z konta są prawdziwe. Od strony sytemu A. J. nie widziała żadnych blokad. Wówczas zawiadomiła telefonicznie departament bezpieczeństwa informując, że ma zgłoszenie od klienta i departament bezpieczeństwa zablokował całe konto klienta. (zeznania świadka A. J. (1) k. 191 – 192)

Reklamację powoda rozpoznawał pracownik pozwanego M. W.. Przed rozmową z klientem przeprowadzono analizę, co do możliwego ataku przez hakerów na urządzenia klienta oraz zaistniało podejrzenie, że powód mógł mieć wirusa w komputerze. Pracownik ten sprawdził logi systemowe (to zdarzenia mające miejsce na rachunku klienta po zalogowaniu się do jego serwisu, wiadomości sms wysłane do klienta w celu dokonania operacji) i sms. Z analizy tej wynikało, że doszło do prawidłowego logowania przez klienta tj. z numeru klienta i przy użyciu hasła należącego do klienta, a następnie zostało wprowadzone hasło, które bank wysłał sms na telefon klienta. Były to dwa hasła: pierwsze do zalogowania, drugie do zmiany odbiorcy zdefiniowanego. W ramach załatwienia reklamacji poproszono T. P. (1), by przeskanował komputer kilkoma różnymi programami antywirusowymi i dokonał zmiany hasła. (zeznania świadka M. W. k. 228 - 232)

Powód, niezwłocznie po przekazaniu przez pozwany bank środków finansowych z jego rachunku bankowego M. A. nieuprawnionej osobie zlecił firmie (...) Komputerowe analizę posiadanego sprzętu komputerowego, tj. notebooka D. (...) za pośrednictwem, którego dokonywał logowania do rachunku M. A.. Komputer powoda posiadał zainstalowany legalny system operacyjny W. (...) oraz oprogramowanie (...) (data instalacji 15.11.2013), a na samym sprzęcie nie wykryto obecności wirusów ani oprogramowania szpiegowskiego. Komputer, z którego powód dokonał logowania do systemu transakcyjnego pozwanego był zabezpieczony w sposób należyty programem antywirusowym. Powód nie udostępniał również nikomu loginu i hasła do tego systemu, jak również nie miało miejsca włamanie do jego miejsca zamieszkania. Powód posługiwał się komputerem posiadającym legalne oprogramowanie oraz system antywirusowy. Korzystał z zakupów internetowych dokonując płatności przez PayU, który przekierowuje powoda na stronę mBanku i loguje się na prawidłowej stronie banku. (orzeczenie z dnia 27 stycznia 2014 r. k. 53)

Bank zamieszczał na stronie internetowej informacje o istniejących zagrożeniach ze strony hakerów np., że może pojawić się na stronie nakładka o połączeniu banku i aby nie potwierdzać jej jednorazowym smsem (w dniu 10.12.2013 r.), o możliwości instalacji programu na telefonie komórkowym. Informacje o nowych sposobach hakerów były również przekazywane mailowo do placówek banku, przy czym nie było pewności czy zostały uwzględnione wszystkie placówki. (zeznania świadka M. W. k. 228 - 232)

W dniu 22 stycznia 2014 r. powód zawiadomił Komisariat IX Policji w G., który wszczął dochodzenie o przestępstwo z art. 279§ l kk, nadzorowane przez Prokuraturę Rejonową G. - O. pod sygn. akt: 2 Ds. 489 /14. Osoba, na rzecz której pozwany bank przekazał środki pieniężne z rachunku powoda bez zlecenia powoda - J. P. sądził, iż wykonuje zadanie testowe na poczet przyszłego zatrudnienia i dla przyszłego pracodawcy spółki (...) credit sp. z o.o.". W ramach owego zlecenia testowego otrzymane z rachunku powoda środki przekazał dwoma przekazami Western U. na Ukrainę: pierwszy przelew dnia 21 stycznia 2014 roku na nazwisko A. M. kwotę 15.973,00, natomiast drugi przelew wykonał dnia 22 stycznia 2014 roku ok. godz. 9:00 na nazwisko A. V. 7.903 zł, pozostała kwota miała być wynagrodzeniem J. P.. J. P. odnalazł ogłoszenie o pracę ww. spółki na stronie gazetapraca.pl. (...) to zostało umieszczone przez podmiot posługujący się adresem IP 46.37.184.51, którego dysponentem jest firma w Wielkiej Brytanii. Postanowieniem z dnia 21 lipca 2014 r. umorzono postępowanie w sprawie wobec nie wykrycia sprawców przestępstwa. (dokumenty z akt sprawy 2 Ds. 489/14: zawiadomienie z dnia 20 lutego 2014 r. k. 130 - 132, notatka z dnia 22.01.20 14 r. k. 120, protokół z przyjęcia ustnego zawiadomienia o przestępstwie k. 121 - 124, notatka urzędowa z dnia 23 stycznia 2014 roku k. 125, pismo pozwanego banku z dnia 28 marca 2014 roku - k. 126 – 127, wydruk k.128, protokół przyjęcia

ustnego zawiadomienia o przestępstwie (J. P.) z dnia 22 stycznia 2014 r. k. 130-132, wydruk potwierdzenia operacji Western U. z dnia 22.01.2014r. k. 133,protokół przesłuchania świadka J. P. k.134, wydruki e – mail dot. J. P. k. 36 -47;.postanowienie prokuratury w przedmiocie zebrania dowodów co do ogłoszenia w gazeta.pl k. 148 – 150, Raport N. k.162 – 163 i 164, notatka urzędowa z dnia 18 czerwca 2014 roku k.167)

Pozwany bank nie weryfikuje adresu IP, ponieważ jest to dana zmienna, klient z rożnych urządzeń może dokonywać logowania. Daną identyfikacyjną dla banku jest numer klienta i jego hasło. Bank nie jest informowany w żaden sposób, o tym że klient np. dokonuje logowania z Europy, a 5 minut później z A.. Niektórzy dostawcy europejscy Internetu mogą mieć firmy zarejestrowane na innym kontynencie. Alert pojawia się jedynie w przypadku IP, o którym ze (...) Banków (...) albo z innego banku jest informacja, że próbowano dokonać przestępstwa wówczas pojawia się alert i takie IP jest blokowane i dodawane na „czarną listę".

Do zalogowania potrzebna jest zarówno znajomość hasła jak i loginu. (...) wymaga podania całego hasła, nie ma maskowania hasła. Bank nie prowadził statystyki transakcji dokonywanych przez klienta i nie był alertowany o transakcji odbiegającej od poprzednich. Bank nie sprawdza danych beneficjenta przelewu, dla banku decydujący jest numer konta.

Przelewy własne można dokonywać przez opcję definicję odbiorcy zaufanego lub nie, lub po zalogowaniu się do serwisu przez przelew własny, który nie wymaga dodatkowej autoryzacji. Nawet gdy jest ustawiona definicja odbiorcy zaufanego w dalszym ciągu można dokonać przelewu własnego. Standardowym ustawieniem jest przelew własny bez autoryzacji, u powoda był to przelew zdefiniowany nie wymagający autoryzacji czyli odbiorca zaufany.

(zeznania świadka M. W. k. 228 - 232)

Powód w dniu 21 stycznia 2014 r. złożył pozwanemu ustną dyspozycję poprzez system telefonicznej rejestracji wypłaty na jego rzecz kwoty 24.296,40 zł, która to dyspozycja nie została wykonana. Następnie pismem z dnia 16 czerwca 2014 r. powód wezwał pozwanego do polubownego zakończenia przedmiotowej sprawy oraz do zapłaty, (zeznania powoda k. 187 – 190 w zw. z k. 252, kopia pisma z dnia 16 czerwca 2014 r. wraz z dowodem nadania k. 54 - 56, nagrania rozmów – płyta k. 94)

Pozwany bank nie rozpatrzył reklamacji powoda z dnia 22 stycznia 2014 r. dotyczącej przekazania środków finansowych powoda na rzecz osoby nieuprawnionej oraz nie odpowiedział na wezwanie do zapłaty (wydruk wiadomości e-mail z dnia 22 stycznia 2014 r. k. 59, wydruk wiadomości e-mail z dnia 21 lutego 2014 r. k. 52, zeznania powoda k. 187 – 190 w zw. z k. 252***)***

Powyższy stan faktyczny Sąd ustalił na podstawie zeznań powoda i świadków A. J. (1) i M. W. oraz dokumentów znajdujących się w aktach sprawy w 2 Ds. 489/14: zawiadomienia z dnia 20 lutego 2014 r., notatki z dnia 22.01.2014r., protokołu z przyjęcia ustnego zawiadomienia o przestępstwie, notatki urzędowej z dnia 23 stycznia 2014 roku, pisma pozwanego banku z dnia 28 marca 2014 roku, protokołu przyjęcia ustnego zawiadomienia o przestępstwie (J. P.) z dnia 22 stycznia 2014 r., wydruku potwierdzenia operacji Western U. z dnia 22.01.2014 r., protokołu przesłuchania świadka J. P., wydruków e – mail dot. J. P.; postanowień prokuratury w przedmiocie zebrania dowodów co do ogłoszenia w gazeta.pl raportów N., notatki urzędowej z dnia 18 czerwca 2014 roku.

Sąd pominął zeznania M. W. w zakresie w jakim opisywał sposób działania hackerów w okresie na przełomie listopada 2013 r. do marca 2014 r., gdyż ten modus operandi nie odpowiadał sposobowi, w jaki niezidentyfikowana osoba włamała się do konta powoda.

Sąd uznał za niewiarygodne zeznania świadka M. W., który utrzymywał, jakoby komputer klienta był zainfekowany szkodliwym oprogramowaniem. Przeczą temu zeznania powoda, gdyż system antywirusowy jak również pozostałe aplikacje, instalował powodowi informatyk, a powód korzysta z niewielkiej ilości programów, na stronę banku logował się zawsze przez zapamiętaną zakładkę i nie pojawił mu się nigdy komunikat o łączeniu się banków, co przeczy możliwości włamania się w ten sposób do konta przed podanie kodu przez klienta banku. Zeznania

świadka pozostają w sprzeczności z orzeczeniem z dnia 27 stycznia 2014 r. o stanie notebooka powoda, istotne, ponieważ dokonane niezwłocznie po zdarzeniu, z którego wynika komputer, z którego powód dokonał logowania do systemu transakcyjnego pozwanego był zabezpieczony w sposób należyty programem antywirusowym. Orzeczenie to jest jedynie dokumentem prywatnym, jednakże potwierdza on zeznania powoda, a przede wszystkim pozwany nie udowodnił okoliczności przeciwnej. Wskazać należy, iż powód proponował oględziny komputera pracownikom banku oraz organom ścigania, lecz oba te podmioty nie widziały takiej potrzeby. Przeciwko zeznaniom M. W. świadczy również okoliczność, iż również telefon powoda nie nadaje się do instalacji żadnych aplikacji z zewnątrz, w tym szpiegowskich, gdyż jest telefonem starego typu.

Sąd na wniosek pełnomocnika pozwanego zwrócił się do (...) S.A. o nadesłanie bilingu dla numeru: (...) z okresu 21-23.01.2014r w celu ustalenia czy powód wpisał hasło jednorazowe sms w nakładkę z informacją o połączeniu banków. Jednak wykonanie ustaleń z powyższego okresu nie było już możliwe z uwagi na przekroczenie 12 miesięcznego okresu przechowywania bilingów. Ustalenie to byłoby również niemożliwe z uwagi na możliwość udzielania tego rodzaju informacji wyłącznie sądom karnym. Dlatego Sąd pominął zeznania świadka M. W. w zakresie w jakim zeznawał na okoliczność możliwości przechwytywania sms przez wirus zainstalowany na telefonie np.: udający program antywirusowy, jako scenariusza używanego wcześniej przez hakerów.

Pełnomocnik pozwanego cofnął wniosek o opinię biegłego informatyka.

***Sąd zważył, co następuje:***

Powództwo podlegało uwzględnieniu w całości co do kwoty należności głównej. Oddaleniu podlegało powództwo w zakresie części okresu odsetkowego.

Podstawą prawną powództwa jest art. 725 kc, zgodnie z którym 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.

W razie dokonania wypłaty środków osobie nieuprawnionej, poszkodowanym tą czynnością jest bank, a nie osoba, która zdeponowała środki na rachunku. Zachowuje ona nadal roszczenie o ich zwrot w całości lub w części. Bank może zwolnić się z zobowiązania wynikającego z umowy rachunku bankowego w takim zakresie, w jakim wierzyciel ze świadczenia skorzystał lub też w razie wykazania przesłanek odpowiedzialności kontraktowej posiadacza rachunku (wyrok Sądu Apelacyjnego w Białymstoku w sprawie I ACa 350/03 z 2003-07-03 Orzecznictwo Sądów Apelacyjnych rok 2004, Nr 6, poz. 16, str. 66, Lex nr 81881)

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 wypłaty gotówki nieuprawnionemu przed dokonaniem zgłoszenia bankowi utraty dowodu zawarcia umowy rachunku oszczędnościowego, czeku lub blankietu czeku nie ponosi posiadacz rachunku. W tym zakresie mają zastosowanie ogólne zasady wykonywania zobowiązań, w tym obowiązek banku zachowania podwyższonej, szczególnej staranności (wyrok Sądu Najwyższego z dnia 9 listopada 2005 r., II CK 201/05, LEX nr 311307)

Ryzyko dokonania wypłaty z rachunku bankowego do rak 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. Ustawa o usługach płatniczych przewiduje generalną zasadę, że dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika. Zgodnie z art. 46

ust 1 powołanej ustawy w przypadku wystąpienia nieautoryzowanej transakcji płatniczej, dostawca płatnika jest obowiązany niezwłocznie dokonać na rzecz płatnika zwrotu kwoty nieautoryzowanej transakcji płatniczej albo, w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcją płatnicza.

Bank ponosi względem powoda odpowiedzialność na podstawie art. 471 kc, zgodnie z którym dłużnik obowiązany jest do naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi. Przesłanki muszą wystąpić łącznie: a) niewykonanie bądź nienależyte wykonanie zobowiązania (naruszenie zobowiązania), b) fakt poniesienia szkody, c) związek przyczynowy pomiędzy niewykonaniem bądź nienależytym wykonaniem zobowiązania a szkodą. W niniejszej sprawie powyższe przesłanki zostały spełnione.

Zobowiązanie Banku jako profesjonalnego podmiotu jest determinowane poprzez ustawowe obowiązki wskazane w m.in. w art. 43 ust. 1 pkt. 1, 3,4, 5, Ustawy o usługach płatniczych. W ten sposób zachodzi na siebie zakres odpowiedzialności banku wynikający z umowy i z ustawy. Bank nie wywiązał się z ich wypełnienia w stosunku do powoda. Nie zapewnił, by indywidualne zabezpieczenia instrumentu płatniczego nie były dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Nie zapewnił również stałej dostępności odpowiednich środków pozwalających użytkownikowi na dokonanie zgłoszenia zgodnie z art. 42 ust. 1 pkt 2 ustawy o usługach płatniczych.

Zobowiązanie Banku względem posiadacza rachunku kształtuje również art. 49 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (tekst jednolity Dz.U. Nr 72 z 2002 r., poz. 665 ze zmianami), które zawierają rozwiązanie pozwalające bankowi na swobodne dysponowanie powierzonymi środkami pieniężnymi, nakładając równocześnie obowiązek dołożenia wszelkich starań w zakresie bezpieczeństwa. Art. 50 Prawa bankowego stanowi, iż bank jest zobowiązany do dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Bank nie wykonał należycie tych obowiązków.

Z materiału dowodowego wynika - zeznań świadka M. W. - wynika, że bank nie wdrożył dodatkowych zabezpieczeń kont klientów poprzez maskowanie /częściowe ukrycie hasła/ czy wymuszenia zmiany hasła co jakiś czas, by wyeliminować albo zminimalizować skutki ataku hakerskiego. Pozwany bank poprzestał na ogłaszaniu zagrożeń na swoich stronach internetowych i w ten sposób ostrzegał klientów o możliwych atakach hakerskich i sposobach ich przeprowadzania.

W pozwanym banku przelewy własne można dokonywać przez opcję definicję odbiorcy zaufanego lub nie, lub po zalogowaniu się do serwisu przez przelew własny, który nie wymaga dodatkowej autoryzacji. Do zalogowania potrzebna jest zarówno znajomość hasła jak i loginu. (...) wymaga podania całego hasła, nie ma maskowania hasła. Nawet gdy jest ustawiona definicja odbiorcy zaufanego w dalszym ciągu można dokonać przelewu własnego. Standardowym ustawieniem jest przelew własny bez autoryzacji, u powoda był to przelew zdefiniowany nie wymagający autoryzacji czyli odbiorca zaufany. Przy istnieniu tego rodzaju rozwiązania bank nie zapewnił monitorowania transakcji dokonywanych na rachunkach bankowych w celu wychwytywania transakcji niestandardowych, by upewniać się co do rzetelności, aby w przypadku wątpliwości co do beneficjenta rzeczywistego zablokować transakcję. Nie było również potwierdzania każdej transakcji za pośrednictwem kodu z tokena. Transakcje dokonywane za pośrednictwem systemu bankowości elektronicznej pozwanego banku wymagały potwierdzenia za pośrednictwem jednego kodu z przesłanej wiadomości na numer telefonu komórkowego posiadacza rachunku. W tej sytuacji przechwycenie przez hakera jednej wiadomości sms zawierającej kod potwierdzający operację ustanowienia odbiorcy zdefiniowanego powodowało możność przekazania temu odbiorcy wszelkich środków posiadanych przez tę osobę bez konieczności dodatkowej weryfikacji takich przelewów.

Rozpoznając reklamację powoda nie wziął pod uwagę przy rozpoznawaniu jego reklamacji okoliczności, iż ok. godz. 14 w dniu 21 stycznia 2014 r. powód zgłaszał pozwanemu – przez A. J. (3) – fakt wyrzucania ze strony internetowej banku. W chwili zgłoszenia i później w trakcie rozpatrywania reklamacji uznano, że błąd dotyczy komputera klienta.

Rozpatrując przypadek powoda Bank opierał się na przypuszczeniach polegających na przypasowaniu zdarzenia do najbardziej zbliżonego do owego przypadku scenariuszach ataku hakerskiego. Z tym, że przyjął, iż wina za spowodowanie tego nieautoryzowanego przelewu leży po stronie klienta banku poprzez niedołożenie należytej staranności, czemu dał wyraz pełnomocnik pozwanego w sprzeciwie od nakazu zapłaty.

Sąd nie podziela stanowiska pozwanego, iż powód jako klient banku naruszył obowiązki wskutek rażącego niedbalstwa wynikające z umowy. Pełnomocnik pozwanego powołał się na § 41 ust. 1 regulaminu otwierania i prowadzenia rachunków oszczędnościowych - rozliczeniowych i oszczędnościowych, przewidującego enumeratywnie wyliczone sposoby zabezpieczeń narzędzi i urządzeń, z których korzysta w celu uzyskania dostępu do rachunku. Regulamin wiąże strony, co wynika z § 7 umowy o świadczenie usług z 2010 r. Należy jednak podnieść, że wymóg § 41 ust. 1 regulaminu przewidujący pobranie aplikacji mobilnej w sposób wskazany przez Bank za pośrednictwem strony internetowej Banku, jest w stosunku do powoda nieadekwatny, ponieważ, jak wynika z zeznań powoda nie korzystał on z aplikacji mobilnych, posiadając stary model telefonu.

Podkreślić także należy, iż było to zawyżonym wymogiem w stosunku do rozwiązań ustawowych. Oznaczałoby to, że powoda dyskwalifikuje fakt posiadania starego typu telefonu, na którym nie można zainstalować zalecanej aplikacji, przy spełnieniu wszystkich pozostałych wymagań dotyczących należytego zabezpieczenia narzędzi i urządzeń w celu uzyskania dostępu do rachunku. Należy podkreślić, iż zgodnie z treścią art. 8 ust. 1 - 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 korzystnej regulacji niż ustawowa stanowi naruszenie art. 8 ust. 1 Ustawy o usługach płatniczych, prowadząc do nieważności regulaminowych postanowień.

W dalszej kolejności pełnomocnik pozwanego podnosił, że z pewnością jedną z przyczyn włamania się do konta klienta było korzystanie ze sklepów internetowych i dokonywanie płatności w nich, co pozwalało na zastosowanie zjawiska tzw. phisingu. Jak dalej podaje pełnomocnik pozwanego, kierując się stanowiskiem Komisji Nadzoru Finansowego z dnia 18 listopada 2013 roku, „niektóre sklepy internetowe umożliwiają nabywcom płatność zgodnie z następującym schematem: po dokonaniu zakupu towaru lub usługi na platformie internetowej i przejściu do etapu płatności, klient jest przekierowywany na stronę pośrednika, gdzie podaje dane do logowania do własnego rachunku bankowego (login/identyfikator oraz hasło). Skutkiem opisywanego powyżej zjawiska jest w świetle komunikatu Komisji Nadzoru Finansowego wystąpienie ryzyka: naruszenia umowy o prowadzenie rachunku bankowego oraz regulaminu, utraty prawa do reklamacji nieautoryzowanych transakcji oraz nieautoryzowanego przechwycenia danych logowania. Stanowisko pozwanego jest chybione, ponieważ powód korzysta w ramach zakupów internetowych z PayU, który przekierowuje na stronę internetową banku i powoduje logowanie na właściwej stronie.

Nie daje też obronić się stanowisko pozwanego odnośnie możliwości skorzystania przez powoda z kierowanych przez hakerów zachęt do użytkowników do „dodatkowego zabezpieczenia telefonu", co miałoby spowodować w dalszej kolejności zainfekowanie szkodliwym oprogramowaniem aparatu komórkowego oraz komputera użytkownika, który umożliwia podejrzenie loginu oraz hasła osobom nieuprawnionym. Z materiału dowodowego wynika niezbicie, że komputer posiadał zainstalowane oprogramowanie (...) i że w dzień dokonania diagnozy, tj. 27 stycznia 2014 roku nie stwierdzono na urządzeniu obecnych wirusów. Za zbyt daleko idące należało uznać rozważania pełnomocnika pozwanego dopuszczające możliwość, aby wirus mógł także zostać usunięty poprzez wykonanie w czasie pomiędzy dokonaniem przelewu a wykonaną ekspertyzą na skutek skanowania notebooka programem antywirusowym. Ponadto pełnomocnik pozwanego cofnął w piśmie procesowym k. 199 – 200 wniosek dowodowy o dopuszczenie opinii biegłego informatyka w zakresie analizy sposobu użytkowania i zabezpieczenia antywirusowego urządzeń należących do powoda, w tym telefonu komórkowego oraz udzielenia wyjaśnień w zakresie możliwego sposobu zainfekowania urządzeń w celu dokonania nieautoryzowanego przelewu, w tym przeanalizowaniu logów w programie antywirusowym notebooka.

Sąd uznał za nietrafną i obliczoną na obronę pozwanego tezę o tym, że wszelkiego rodzaju incydenty dotyczące wyprowadzenia środków z rachunków związane są z przełamaniem zabezpieczeń komputerów klientów. Powód zawiadomił bowiem pozwanego o zaistnieniu nieautoryzowanego przelewu z jego rachunku na rachunek oznaczony jako J. P. w dniu 21 stycznia 2014 r. i domagał się zablokowania tego konta. Mimo to bank zaniechał zablokowania rachunku bankowego J. P. – mógł to wykonać tylko departament bezpieczeństwa, co sprawiło, że osoba ta przekazała bez przeszkód następnego dnia środki powoda na Ukrainę. Należy podkreślić, że powód pierwsze niepokojące komunikaty na rachunku zauważył rano 21 stycznia 2014 r. Również i wówczas zgłoszona reklamacja została przez pracownika pozwanego zbagatelizowana. Szczególnie niepokojący w tej sprawie był brak możliwości przeciwdziałania dokonywanym nielegalnie przelewom na koncie i z konta powoda w obrębie bankowego systemu internetowego powoda niezwłocznie w chwili zgłoszenia nieprawidłowości. Możliwa była wówczas jedynie blokada poszczególnych kanałów i dostępów internetowego i sms – owego oraz przyjęcie reklamacji, w ramach której pracownicy infolinii mieli uprawnienie jedynie, żeby złożyć dyspozycję do departamentu bezpieczeństwa. Zgłoszenie reklamacji miało miejsce 21 stycznia 2014 r. o godz. 23, a możliwość blokady rachunków z uwagi na sposób funkcjonowania departamentu bezpieczeństwa nastąpiło dopiero rano następnego dnia. Brak funkcjonowania tego kluczowego departamentu w godzinach nocnych spowodował, że Bank nie zareagował stosownie do zagrożenia i nie zabezpieczył środków finansowych powoda. Dlatego twierdzenie, że powód się do tego przyczynił nie jest w żaden sposób usprawiedliwione wobec dokonania przez niego wszystkich aktów staranności. Wynika to jasno z nagrań rozmów przeprowadzonych przez powoda w nocy z 22/23 stycznia 2014 r. z działem infolinii pozwanego.

Powód poniósł szkodę w wysokości 24.296,40 zł wskutek wypłacenia środków osobie nieuprawnionej. Zachodzi związek przyczynowy pomiędzy zachowaniem pozwanego a szkodą powoda. Powód wykonał niezwłocznie wszystkie czynności zmierzające do powiadomienia banku o niebezpieczeństwie nieautoryzowanego użycia jego konta. Kontaktował się telefonicznie z kolejnymi osobami w D. (...) Klienta w ciągu kilkunastu godzin od 21 stycznia do 22 stycznia 2014 r. Czynności tej dokonał na podstawie art. 42 ust. 1 pkt 2 (czyli niezwłocznego zawiadomienia o zaistnieniu nieautoryzowanej transakcji płatniczej).

Stosownie do art. 46 ust. 5 ustawy po usługach płatniczych jeżeli dostawca, wbrew obowiązkowi, o którym mowa w art. 43 ust. 1 pkt 3, nie zapewnia odpowiednich środków umożliwiających dokonanie w każdym czasie zgłoszenia, o którym mowa w art. 42 ust. 1 pkt 2, płatnik nie odpowiada za nieautoryzowane transakcje płatnicze, chyba że płatnik doprowadził umyślnie do nieautoryzowanej transakcji. Natomiast w myśl art. 45 cytowanej ustawy ciężar wykazania, że dana transakcja płatnicza została przez użytkownika autoryzowana lub, że została wykonana prawidłowo spoczywa na dostawcy tego użytkownika, tj. pozwanym (...) S.A., przy czym do udźwignięcia tego ciężaru dowodowego nie jest wystarczające wykazanie samego zarejestrowanego użycia instrumentu płatniczego, (art. 45 ust. 2 ustawy o usługach płatniczych). Pozwany nie uwolnił się od odpowiedzialności, ponieważ nie udowodnił, że powód swoim działaniem doprowadził do nieautoryzowanej transakcji. Przeciwnie postępowanie dowodowe wykazało, że nie dokonał żadnej z czynności związanej z ustanowieniem profilu zaufanego, nie dokonał przelewu środków pomiędzy rachunkiem oszczędnościowym a bieżącym i nie dokonał przelewu na profil zaufany. Dlatego Sąd uznał za niezasadny zarzut przyczynienia się powoda do powstania szkody w 50%. Przede wszystkim nie wykazano, w jako sposób powód miałby się do powstania szkody przyczynić. Zwłaszcza w kontekście dokonanych przez niego niezwłocznie czynności zmierzających do zawiadomienia banku, a z drugiej strony posiadania legalnego oprogramowania i programu antywirusowego.

Mając powyższe na uwadze Sąd zasądził na rzecz powoda dochodzoną kwotę 24.296.40 zł w całości.

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. Istotne jest więc ustalenie momentu, w którym dłużnik opóźnił się ze spełnieniem świadczenia. W tym zakresie uzasadnione było zasądzenie odsetek zgodnie z ogólną regułą art. 455 k.c., według którego świadczenie powinno być spełnione niezwłocznie po wezwaniu dłużnika do wykonania. W dniu 21 stycznia 2014 r. powód złożył dyspozycje wypłaty i

reklamację. Do wezwania do zapłaty datowane na 16 czerwca 2014 r. powód nie załączył dowodu doręczenia, tylko dowód nadania wezwania, co nie pozwala ustalić dokładnie kiedy pozwany je odebrał. Za pierwsze wezwanie do zapłaty sprecyzowanej kwoty należy uznać pozew, dlatego też Sąd – zgodnie zasądził odsetki dopiero od dnia następującego po dniu doręczenia pozwanemu odpisu pozwu (k. 61) – tj. od dnia 31.10.2014 do dnia zapłaty. Żądanie powoda zasądzenia odsetek od daty wcześniejszej było nieudowodnione i jako takie podlegało oddaleniu.

Sąd orzekł o kosztach procesu na podstawie art. 100 zd. 2 kpc, uznając, że powód uległ jedynie nieznacznej części swych roszczeń (jedynie w zakresie części roszczenia odsetkowego) i zasądził od pozwanego na rzecz powódki kwotę 3.632 zł stanowiącą koszty poniesione przez powódkę w toku procesu, na którą złożyły się: 1215 zł- opłata sądowa, 2400 zł- wynagrodzenie dla pełnomocnika (ustalone na podstawie § 6 ust. 5 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.) oraz 17 zł – opłata skarbowa od pełnomocnictwa.