Sygnatura akt XI C 1225/21

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

W., dnia 20 kwietnia 2023 r.

Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu XI Wydział Cywilny w następującym składzie:

Przewodniczący: SSR Anna Małecka

Protokolant: Agnieszka Ryndak

po rozpoznaniu w dniu 20 kwietnia 2023 r. we Wrocławiu

na rozprawie

sprawy z powództwa A. W.

przeciwko (...) Bankowi (...) S.A. z siedzibą w K.

o ustalenie i nakazanie

ustala, że stosunek prawny wynikający z umowy o limit zadłużenia w koncie numer (...) z dnia 17 września 2021 r. między stroną pozwaną (...) Bankiem (...) S.A. z siedzibą w K. a powódką A. W. nie istnieje;

oddala powództwo w pozostałym zakresie

zasądza od strony pozwanej na rzecz powódki kwotę 582,34 zł tytułem zwrotu kosztów procesu, wraz z odsetkami ustawowymi za opóźnienie od dnia uprawomocnienia się niniejszego wyroku do dnia zapłaty.

Anna Małecka

Sygnatura akt XI C 1225/21

UZASADNIENIE

Powódka A. W. pozwem z dnia 15 listopada 2021 r. wniosła o ustalenie nieistnienia stosunku prawnego wynikającego z Umowy o limit zadłużenia w koncie (...) zawartej dnia 17 września 2021 r. między powódka a stroną pozwaną (...) Bankiem (...) S.A. oraz o ustalenie, że powódka nie ponosi odpowiedzialności i nie jest zobowiązana do spłaty zobowiązań wobec pozwanego wynikających z dokonania nieautoryzowanych przez powódkę transakcji płatniczych na łączną kwotę 20.000 zł w postaci przelewu z dnia 17 września 2021 r. z rachunku (...) na nr rachunku (...) na kwotę 10.000 zł oraz dziesięciu transakcji BLIK każda na kwotę po 1.000 zł. Ponadto powódka wniosła o nakazanie stronie pozwanej przywrócenie rachunku płatniczego powódki numer (...) do stanu jaki istniałby, gdyby nie miały miejsca wyżej wymienione nieautoryzowane transakcje płatnicze. Jednocześnie powódka wniosła o zasądzenie na jej rzecz kosztów postępowania.

W uzasadnieniu pozwu wskazała, że jest posiadaczką rachunku bankowego o numerze (...) prowadzonego na jej rzecz przez pozwany bank. W dniu 17 września 2021 r. odebrała połączenie telefoniczne z numeru, będącego oficjalnym numerem infolinii (...) Banku (...) S.A. Dzwoniący przedstawił się jako pracownik banku i poinformował powódkę, że zidentyfikowano podejrzane operacje bankowe na rachunku bankowym powódki, tj. zaciągnięcie 3 kredytów i konieczne jest wykonanie procedury zabezpieczenia rachunku bankowego poprzez pobranie wskazanej przez niego aplikacji oraz zalogowanie się do bankowości elektronicznej. Powódka postąpiła według instrukcji osoby dzwoniącej. Wskutek podstępu osoba trzecia w trakcie trwania połączenia telefonicznego dokonała zawarcia bez zgody i wiedzy

powódki Umowy o limit zadłużenia na koncie powódki do kwoty 20.800 zł oraz dokonała nieautoryzowanych przez powódkę transakcji na łączną kwotę 20.000 zł (10.000 zł tytułem przelewu i kolejne 10.000 zł w formie 10 transakcji blik każda po 1.000 zł). Powódka po zakończeniu rozmowy zadzwoniła na numer infolinii banku i została poinformowana, że prawdopodobnie padła ofiarą oszustwa i winna złożyć stosowne zawiadomienie organom ścigania.

Powódka wskazała, że nie zawarła Umowy o limit zadłużenia oraz nie autoryzowała transakcji, które doprowadziły do powstania zadłużenia. Nie jest więc stroną wymienionej umowy kredytowej i nie ponosi odpowiedzialności za dokonane transakcje płatnicze. Powódka nie udostępniła nikomu w sposób świadomy loginu i hasła dostępowego do rachunku bankowego. Przejęcie kontroli nad jej urządzeniem nastąpiło z wykorzystaniem dedykowanego do tego celu oprogramowania sprawcy.

Zdaniem powódki bank nie dołożył należytej staranności w zakresie odpowiedniego zabezpieczenia dostępu do kanału bankowości elektronicznej, w tym nie zapobiegł nietypowym transakcjom na rachunku powódki. Powódka nie przyczyniła się do powstania szkody, jej działania nie noszą znamion umyślności lub rażącego niedbalstwa, nawet gdyby przypisać powódce, iż nie dochowała należytej staranności w zabezpieczeniu własnych interesów bądź nie wykazała się odpowiednią czujnością podczas rozmowy. Okoliczności w jakich bowiem doszło do zdarzenia nie mają charakteru typowych sytuacji, z jakimi przeciętny konsument ma do czynienia na co dzień.

W odpowiedzi na pozew strona pozwana wniosła o oddalenie powództwa w całości oraz zasądzenie na jej rzecz kosztów procesu.

W uzasadnieniu podniosła, że przy zawieraniu przedmiotowej umowy pożyczki nie zostały przełamane żadne zabezpieczenia banku. Transakcje kwestionowane przez powódkę oraz zaciągnięcie pożyczki nastąpiło za pośrednictwem bankowości elektronicznej przy zastosowaniu silnego uwierzytelnienia z wykorzystaniem kodów autoryzacyjnych. Nie jest również zawinieniem ze strony pozwanej „przejęcie, podszycie się" przez oszustów pod infolinię banku – w takim przypadku nie są przełamywane żadne zabezpieczenia banku, lecz sieci komórkowej. Kwestionowana przez powódkę umowa o limit zadłużenia została zawarta za pośrednictwem bankowości elektronicznej po zalogowaniu się z wykorzystaniem danych powódki oraz po dokonaniu autoryzacji kodem przesłanym w wiadomości sms. Przelewy zostały natomiast wykonane zgodnie z zaleceniami (z zastosowaniem silnego uwierzytelnienia). Transakcje te również zostały potwierdzone SMS-em autoryzacyjnym, przesłanym na urządzenie zaufane przypisane do loginu służącego do logowania się do konta bankowego powódki poprzez bankowość elektroniczną. Powyższe wskazuje, że owe transakcje i operacje zostały wykonane przez powódkę lub osoba trzecia jedynie na skutek działania powódki weszła w posiadanie niezbędnych danych oraz urządzenia zaufanego powódki, względnie posiadała kontrolę nad urządzeniem zaufanym powódki.

Powódka przyznała, że skorzystała z nieznanego jej oprogramowania (AnyDesk), którego instalację zleciła jej nieznana osoba trzecia – bez uprzedniej weryfikacji zarówno oprogramowania jak i rozmówcy, pomimo licznych ostrzeżeń banku w tym przedmiocie. Oprogramowanie to umożliwiło oszustowi dostęp do bankowości elektronicznej powódki. Niemniej przed wykonaniem zlecenia pozwana otrzymała na numer telefonu wiadomości SMS-y, w których wyraźnie wskazano co jest przedmiotem autoryzacji (zmiana hasła do bankowości internetowej, podpisanie umowy kredytowej, zlecenie przelewu na kwotę 10.000 zł, zmiana limitów dla transakcji BLIK).

Zdaniem strony pozwanej powódka instalując nieznaną i niezweryfikowaną przez nią aplikację oraz udostępniając osobie trzeciej dane poufne, nie zachowała podstawowych zasad bezpieczeństwa.

Jednocześnie pozwany bank podniósł, że powódka nie ma interesu prawnego w domaganiu się ustalania nieistnienia umowy pożyczki.

Postanowieniem z dnia 17 grudnia 2021 r. sąd sprawdził wartość przedmiotu sporu i ustalił ją na kwotę 40.800 zł.

Sąd ustalił następujący stan faktyczny:

A. W. jest posiadaczką rachunku bankowego numer (...) prowadzonego na jej rzecz przez (...) Bank (...) S.A. z siedzibą w K..

/bezsporne/

W dniu 17 września 2021 r. A. W. odebrała połączenie telefoniczne z numeru telefonu +48 32 357 00 69, który jest tożsamy z numerem infolinii (...) Banku (...) S.A. widniejącym na stronie internetowej banku, lecz powódka nie znała na pamięć tego numeru i widząc numer telefonu przed odebraniem połączenia nie wiedziała, kto inicjuje rozmowę. Osoba dzwoniąca przedstawiła się jako przedstawiciel banku (...) S.A. i poinformowała A. W. o podejrzanych transakcjach na jej rachunku bankowym, w tym, że zaciągnięto na nią zadłużenie. Mężczyzna poprosił w związku z tym o zainstalowanie na telefonie powódki aplikacji AnyDesk, która miała umożliwić połączenie z działem technicznym i finansowym banku, co też A. W. uczyniła. Pobrana aplikacja AnyDesk zgodnie z instrukcją mężczyzny była cały czas uruchomiona w trakcie trwającej rozmowy

Następnie rozmówca powódki poprosił o potwierdzenie danych osobowych, w tym daty urodzenia i numeru PESEL, a potem poinstruował A. W., by ta zmieniła hasło do mobilnej aplikacji bankowości elektronicznej (...), jak i login oraz hasło do strony internetowej, co miało zabezpieczyć konto bankowe przed dostępem osób trzecich.

Po zalogowaniu się na konto bankowe A. W. nie dostrzegła jakichkolwiek zmian stanu środków na koncie, kwoty były takie, jak po wykonaniu ostatniej operacji przez A. W..

W trakcie dalszej rozmowy z mężczyzną na numer telefonu A. W. wysyłano kody autoryzacyjne w formie SMS-ów następującej treści:

- o godzinie 15:28: „ (...) Bank (...), Zmieniasz hasło do bankowości internetowej. Kod do autoryzacji: (...)"",

- o godzinie 15:37: „ (...) Bank (...), Kod autoryzacyjny dla podpisania umowy kredytowej to: (...)"

- o godzinie 15:42: „ (...) Bank (...), Robisz przelew na konto 25xxx120 na kwotę 10.000 złotych. Kod do autoryzacji: (...)",

- o godzinie 15:57: „ (...) Bank (...), Zmieniasz limity transakcyjne dla (...). Kod do autoryzacji: (...)",

- o godzinie 15:59: „ (...) Bank (...), Kod autoryzacyjny dla zmiany limitów transakcyjnych dla karty: (...) to (...)".

/dowód:

- przesłuchanie powódki, protokół rozprawy z 26.05.2022 r. 00:02-00:53, k. 149-150,

- wykaz logów wysyłanych do powódki smsów, k. 92-95./

Powódka odczytywała SMS-y po ich otrzymaniu; nadejście SMS-ów oraz ich treść nie wzbudzały podejrzeń A. W., gdyż jej rozmówca poinformował ją wcześniej, że będą przychodzić SMS-y, co jest konieczne dla zabezpieczenia jej finansów.

Na skutek działań osoby trzeciej za pomocą bankowości elektronicznej doszło do zawarcia umowy o limit zadłużenia w koncie (...) na kwotę 20.800 złotych, gdzie między A. W. jako pożyczkobiorcą (...) Bankiem (...) S.A. jako pożyczkodawcą.

/dowód:

- umowa o limit zadłużenia w koncie (...), k. 16-28

- wykaz logów wysyłanych do powódki smsów, k. 92-95

- przesłuchanie powódki, protokół rozprawy z 26.05.2022 r. 00:02-00:53, k. 149-150./

Następnie z rachunku bankowego A. W. wykonano przelew na kwotę 10.000 zł na rachunek należący do M. B. o numerze (...). A. W. nie na M. B., później dowiedziała się, że rachunek tej osoby został wykorzystany przez nieuprawnione osoby trzecie.

/dowód:

- potwierdzenie przelewu na kwotę 10.000 zł, k. 30,

- wykaz logów, k. 92-95,

- przesłuchanie powódki, protokół rozprawy z 26.05.2022 r. 00:02-00:53, k. 149-150./

Rozmówca powódki nakazał jej uruchomić operację BLIK w aplikacji bankowej a po wygenerowaniu kodów BLIK odczytywać je na głos.

Rachunek bankowy A. W. został obciążony poprzez dokonanie 10 wypłat z bankomatu w kwocie po 1.000 zł każda. Środki pieniężne były wypłacone w bankomacie (...), znajdującym się przy ul. (...) w W., za pomocą kodów BLIK, które zostały wpisane na klawiaturze bankomatu, a ponadto zaakceptowane w aplikacji mobilnej poprzez podanie (...)u na urządzeniu H. (...) , który znajduje się na liście urządzeń zaufanych A. W..

Na skutek dokonanych transakcji na rachunku bieżącym powódki o numerze (...) powstał debet w wysokości 20.000 zł.

/dowód:

- wydruki potwierdzenia wykonania transakcji BLIK, k. 31-40,

- wykaz logów, 93-95

- zeznania świadka W. M., protokół rozprawy z 7.03.2022 r., 00:08-01:02, k. 146-147,

- przesłuchanie powódki, protokół rozprawy z 26.05.2022 r., 00:02-00:53, k. 149-150./

Połączenie telefoniczne powódki z mężczyzną przedstawiającym się jako pracownik (...) Banku (...) S.A. trwało około 1 godziny, aż zostało bez uprzedzenia przerwane. W związku z tym A. W. oddzwoniła na ten sam numer telefonu i dodzwoniła się na infolinię (...) Banku (...) S.A., została połączona z konsultantką banku. Została wówczas poinformowana, że najprawdopodobniej padła ofiarą oszustwa, a mężczyzna, z którym rozmawiała, nie jest pracownikiem banku. Konsultantka zabezpieczyła konto A. W. i poprosiła o zastrzeżenie dowodu osobistego.

A. W. złożyła telefonicznie reklamację. Nie zdarzyło jej się wcześniej by ktoś wykorzystał jej dane osobowe, nie zgubiła dokumentów.

Reklamacja A. W. nie została uwzględniona, o czym została poinformowana pismem z 6 października 2021 r.

/dowód:

- pismo (...) Banku (...) S.A. z 6.10.2021 r., k. 42-51

- przesłuchanie powódki, protokół rozprawy z 26.05.2022 r., 00:02-00:53, k. 149-150./

A. W. złożyła zawiadomienie o możliwości popełnienia przestępstwa. Postępowanie przygotowawcze na skutek nie wykrycia sprawcy zostało umorzone.

/dowód:

- potwierdzenie złożenia zawiadomienia, k. 53- 56,

- pismo Prokuratury Rejonowej W. z 27.07.2022 r., k. 154./

A. W. we wrześniu 2021 r. miała 25 lat, absolwentką studiów ekonomicznych, ma tytuł magistra zarządzania jakością .

/dowód: przesłuchanie powódki, protokół rozprawy z 26.05.2022 r., 00:02-00:53, k. 149-150/

Zgodnie z § 11 ust. 1 Regulamin świadczenia usług (...) bankowości internetowej (...) Banku (...) S.A. autoryzacja zlecenia płatniczego przez użytkownika oznacza jego zgodę na wykonanie transakcji płatniczej. Natomiast w myśl § 11 ust. 2 pkt 3 Regulaminu autoryzacja dyspozycji, we tym zleceń płatniczych składanych przez użytkownika za pomocą Systemu bankowości internetowej, w tym aplikacji mobilnej obejmuje: podanie poprawnego kodu lub kodów autoryzacyjnych i wybranie przycisku akceptacji – gdy Bank uzna, że dana dyspozycja płatnicza, ze względu na przepisy prawa lub zasady bezpieczeństwa, wymaga autoryzacji przez podanie kodu lub kodów autoryzacyjnych. Bank dostarcza użytkownikowi kody autoryzacyjne, które są kodami SMS, w wiadomości SMS na wskazany wcześniej przez użytkownika telefon do autoryzacji.

Postanowienie § 34 ust. 9 Regulaminu świadczenia usług (...) bankowości internetowej (...) Banku (...) S.A. stanowi, iż użytkownik zobowiązuje się przechowywać zaufane urządzenie mobilne z zachowaniem należytej staranności, tak aby nie dopuścić do logowania osób trzecich do systemu, w tym do aplikacji mobilnej.

/dowód: Regulamin świadczenia usług (...) bankowości internetowej (...) Banku (...) S.A., k. 96-111/

Klient, aby móc korzystać z bankowości elektronicznej (...) Banku (...) S.A., musi posiadać login hasło oraz telefon, z którego może obsługiwać SMS-y autoryzacyjne. By zalogować się do bankowość elektronicznej musi podać login oraz 5 losowych znaków z ustalonego hasła. Aby używać bankowość mobilnej należy podczas pierwszego logowania podać login, 5 losowych znaków ustalonego hasła, numer PESEL, kod sms który potwierdza ustawienie (...)u; jeśli telefon ma taką możliwość można logować się biometrycznie przez przycisk palca. Kolejno każdorazowe używanie aplikacji mobilnej odbywa się poprzez podanie kodu (...) . Kodem SMS są zabezpieczone dodatkowe funkcje.

(...) Bank (...) S.A. posiada system monitoringu zdarzeń w bankowości internetowej: system zawiera algorytmy, które mają wykrywać ryzykowne lub podejrzane operacje. Bank dysponuje możliwością odrzucenia takiej transakcji lub zablokowania jej.

/dowód: zeznania świadka W. M., protokół rozprawy z 7.03.2022 r., 00:08-01:02, k. 146-147/

(...) Bank (...) S.A. przed 17 września 2021 r. wysyłał do swoich klientów, w tym A. W. komunikaty o zagrożeniach płynących z posiadania bankowości elektronicznej.

Na stronie internetowej banku http: www.ing.pl/aktualności/bankowość-elektroniczna publikowane są informacje mające na celu uświadomienie użytkownikom różnych technik stosowanych przez przestępców. W dniu 30 października 2020 r. opublikowano komunikat: „Oszuści dzwonią z numerów podszywających się pod infolinię banku".

/dowód:

- wykaz komunikatów bezpieczeństwa publikowanych przez (...) Bank (...) w bankowości elektronicznej powódki, k. 129-132,

- wydruk z komunikatów zawartych na stronie internetowej (...) Banku (...) z 30.20.2020 r., k. 112-118,

- zeznania świadka W. M., protokół rozprawy z 7.03.2022 r., 00:08-01:02, k. 146-147./

Stan faktyczny sąd ustalił w oparciu o dowody z przesłuchania powódki, zeznania świadka W. M.. Należy wskazać, że zaistniały stan sprawy co do zasady nie był między stronami sporny i znalazł on również potwierdzenie w pozostałym materiałem dowodowym w sprawie, w tym w przedłożonych przez strony dokumentach , których autentyczności żadna ze stron nie podważała (m.in. wydruku umowy na limit kredytowy, wydrukach potwierdzeń przelewu, wykazie logów z bankowości elektronicznej). Sąd ustalając stan faktyczny oparł się również na treści wiadomości sms, które A. W. otrzymywała w dniu 17 września 2021 r., a które potwierdzają przebieg wydarzeń z 17 września 2021 r. i istnienie spornych transakcji.

Dowody w postaci przedłożonych dokumentów (Regulamin świadczenia usług systemu bankowości internetowej (...) Banku (...) S.A. w brzmieniu na dzień 17 września 2021 r., zrzuty ekranu obrazujące komunikaty bezpieczeństwa widniejące na stronie internetowej banku także nie budziły wątpliwości co ich autentyczności oraz istnienia w dacie 17 września 2021 r.

Sąd pominął dowód z opinii biegłego z zakresu informatyki na podstawie art. 235^2 § 1 pkt 2 k.p.c., gdyż dowód ten zmierzał do wykazania faktu w istocie bezspornego. Powódka bowiem nie kwestionowała, że na skutek rozmowy z osobą podającą się za pracownika banku, na swoim telefonie dokonała instalacji oprogramowania AnyDesk, który umożliwił osobie trzeciej wgląd w zawartość jej telefonu, w tym zapoznanie się z kodami autoryzującymi dokonane transakcje, a także loginem i hasłem do bankowości elektronicznej. Podobnie powódka nie negowała, że otrzymywała wiadomości SMS wysyłane przez stronę pozwaną (przytoczyła ich treść w trakcie przesłuchania na rozprawie w dniu 26 maja 2022 r.). Natomiast kwestia czy wymienione oprogramowanie pochodziło z legalnego źródła czy było aktualne oraz czy powódka miała zainstalowany program antywirusowy nie miały istotnego znaczenia dla niniejszej sprawy.

Sąd zważył, co następuje:

Powództwo zasługiwało jedynie częściowo na uwzględnienie, to jest w zakresie żądania ustalenia nieistnienia stosunku prawnego wynikającego z Umowy o limit zadłużenia w koncie o numerze (...).

Zgodnie z przepisem art. 189 k.p.c. powód może żądać ustalenia przez sąd istnienia lub nieistnienia stosunku prawnego lub prawa, gdy ma w tym interes prawny. Interes prawny w rozumieniu przywołanego przepisu zachodzi wówczas, gdy sam skutek, jaki wywoła uprawomocnienie się wyroku ustalającego, zapewni powodowi ochronę jego prawnie chronionych interesów, czyli definitywnie zakończy spór istniejący lub prewencyjnie zapobiegnie powstaniu takiego sporu w przyszłości, a jednocześnie interes ten nie podlega ochronie w drodze innego środka.

W myśl art. 720 § 1 k.c. przez umowę pożyczki dający pożyczkę zobowiązuje się przenieść na własność biorącego określoną ilość pieniędzy albo rzeczy oznaczonych tylko co do gatunku, a biorący zobowiązuje się zwrócić tę samą ilość pieniędzy albo tę samą ilość rzeczy tego samego gatunku i tej samej jakości. Pożyczka jest umową konsensualną, polegającą na zgodnym oświadczeniu woli stron, dającego i biorącego pożyczkę.

Wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny (art. 60 k.c.), w tym również przez ujawnienie tej woli w postaci elektronicznej. Niezbędnymi składnikami oświadczenia woli są wola i jej wyraz (uzewnętrznienie). To, czy w danym przypadku dochodzi do oświadczenia woli zależy od tego, czy wola zostaje wyrażona ale także i od tego, czy dany podmiot ma świadomość tego i chce, by to co oświadcza było traktowane jako jego oświadczenie woli, które ma wywoływać określone skutki w sferze stosunków cywilnoprawnych (wyrok SN z 23.1.2003 r., sygn. III RN 6/02). Celem oświadczenia jest zakomunikowanie innym osobom woli składającego, dlatego jego treść powinna odpowiadać woli wewnętrznej osoby składającej to oświadczenie. Nie będzie zatem oświadczeniem woli zachowanie podmiotu, z którego wynika brak zamiaru wywołania jakichkolwiek skutków prawnych (S. Rudnicki, Komentarz do Kodeksu Cywilnego, Księga I, 2009 r.).

Prawo bankowe dopuszcza składanie oświadczeń woli związanych z dokonywaniem czynności bankowych w postaci elektronicznej, stanowiąc przy tym, że czynność dokonana w tej formie spełnia wymagania formy pisemnej, w tym formy pisemnej zastrzeżonej pod rygorem nieważności (art. 7 ust. 1 i 3 Prawa bankowego). Jednakże czynność mająca na celu uzewnętrznienie oświadczenia woli musi pochodzić bezpośrednio od osoby, która zamierza danej czynności prawnej dokonać. Osoba ta musi przejawiać świadomość i zamiar dokonania określonej czynności prawnej, winna podjąć skonkretyzowane działanie, zmierzające do celu, jakim jest wstąpienie w dany stosunek prawny, np. stosunek zobowiązaniowy. Innymi słowy: musi przedsięwziąć zachowanie skierowanego na wywołanie zamierzonego przez stronę skutku prawnego, związanego z dokonywaną czynnością.

W przedmiotowej sprawie zabrakło omawianych elementów oświadczenia woli po stronie powódki, dlatego też brak jest podstaw do uznania, że przyjęła ona ofertę banku zawarcia umowy pożyczki (umowy o limit zadłużenia). Powódka niewątpliwie nie miała woli zawarcia umowy o limit zadłużenia w koncie (...) 6110 dnia 17 września 2021 r. Wbrew twierdzeniom strony pozwanej nie złożyła świadomie oświadczenia woli, które skutkowałoby zawarciem umowy o limit zadłużenia ze stroną pozwaną. Nie podjęła działań ukierunkowanych na zawarcie tej umowy. Wszelkie czynności elektroniczne, które doprowadziły do uruchomienia na rachunku bankowym powódki limitu zadłużenia, zostały dokonane bez wiedzy i wbrew jej woli przez nieznane osoby trzecie, które uzyskały dostęp do konta internetowego powódki w (...) Banku (...) S.A.

Z ustaleń poczynionych w sprawie wynika, co prawda, że w bankowości elektronicznej powódki wygenerowano wniosek o zawarcie umowy i potwierdzono kodem autoryzacyjnym jej zawarcie, jednakże A. W. nie uczyniła tego intencjonalnie i świadomie. Powódka w chwili zawierania umowy pozostawała w mylnym przekonaniu, że rozmawia z pracownikiem obsługi technicznej (...) Banku (...) S.A., zaś bank podejmuje działania zmierzające do ustalenia, w jaki sposób osoba trzecia uzyskała dostęp do jej rachunku bankowego, a także mające na celu zabezpieczenie jej rachunku bankowego. Okoliczność, iż przekonanie powódki już w chwili otrzymania SMS-ów dotyczących umowy należy uznać na nieuzasadnione nie powoduje, że można jej przypisać złożenie woli przez zaniechanie podjęcia stosownych działań w tamtym momencie. Powódka nie miała woli zawarcia umowy pożyczki; czynności które do tego doprowadziły, a w których uczestniczyła powódka nie były objętej jej wolą wywołania skutku w postaci zawarcia umowy o limit zadłużenia.

Powódka posiada zatem interes prawny w ustaleniu, że pomiędzy nią, a stroną pozwaną nie istnieje stosunek zobowiązaniowy wynikający z umowy o limit zadłużenia w koncie (...). A. W. nie może w inny sposób, niż w drodze powództwa opartego o art. 189 k.p.c. uzyskać orzeczenie stwierdzające brak stosunku zobowiązaniowego łączącego ją ze stroną pozwaną w związku z umową o limit zadłużenia. Należy podkreślić, iż przepisy art. 42-46 ustawy z dna 19 sierpnia 2011 o usługach płatniczych mają charakter irrelewantny dla rozstrzygnięcia niniejszej kwestii. Wskazać bowiem należy, że zaciągnięcie pożyczki drogą elektroniczną, w tym wypadku umowy o limit zadłużenia, nie stanowi transakcji płatniczej w rozumieniu przepisów ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych. Zgodnie z art. 2 pkt 29 ustawy transakcja płatnicza oznacza zainicjowaną przez płatnika lub odbiorcę wpłatę, transfer lub wypłatę środków pieniężnych.

Konkludując, w świetle dowodów przedłożonych do akt sprawy i okoliczności faktycznych ujawnionych w toku postępowania nie ulega wątpliwości, że powódka dnia 17 września 2021 r. nie złożyła wobec (...) Banku (...) S.A. oświadczenia woli skutkującego zawarciem umowy o limit zadłużenia na koncie (...) , wobec czego w punkcie I wyroku sąd ustalił, że pomiędzy powódką i stroną pozwaną nie istnieje stosunek zobowiązaniowy wynikający z umowy o limit zadłużenia na koncie (...) z dnia 117 września 2021 r.

Orzeczenie to nie rozstrzyga możliwości dochodzenia przez bank zwrotu przekazanych na rachunek powódki środków, np. w oparciu o przepisy art. 405 i nast. k.c.

Pozostałe objęte pozwem roszczenia powódki nie zasługiwały na uwzględnienie.

Strony łączyła umowa rachunku bankowego. Zgodnie z treścią 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; na banku spoczywa obowiązek zwrotu wolnych środków pieniężnych na każde żądanie, chyba że umowa uzależnia obowiązek zwrotu od wypowiedzenia. Prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych oraz zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych określa ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (tj. Dz.U. z 2022 r. poz. 2360), która kompleksowo reguluje rynek usług płatniczych normując zasady podejmowania i prowadzenia działalności na rynku usług płatniczych przez dostawców wskazanych w art. 4 ust. 2, jak i prawa i obowiązki dostawców usług płatniczych związane ze świadczeniem usług płatniczych (Barbara Bajor, Jan Brylski, Anna Zalcewicz, Ustawa o usługach płatniczych. Komentarz, wyd. II. LEX 2017).

Zgodnie z art. 40 przywołanej ustawy autoryzacja transakcji oznacza wyrażenie zgody na dokonanie transakcji płatniczej, czyli stanowi oświadczenie woli użytkownika składane z zamiarem i świadomością wywołania określonych skutków prawnych, tj. dokonania transakcji płatniczej. Sposób wyrażenia zgody (czyli sposób autoryzacji transakcji) jest uzależniony od rodzaju transakcji płatniczej, wykorzystywanego instrumentu płatniczego czy sposobu zlecania usługi płatniczej (w formie papierowej czy drogą elektroniczną). Sposób autoryzowania transakcji określony jest w załączonych do umowy ramowej regulaminach wskazujących, w jaki sposób dochodzi do autoryzacji transakcji (np. przez wpisanie kodu autoryzacyjnego otrzymywanego w wiadomości sms). Prawidłowa, zgodna z określonymi w załączonych do umowy ramowej regulaminami, autoryzacja jest zasadniczym elementem w procesie przeprowadzania transakcji. Przede wszystkim od ustalenia, czy doszło do autoryzacji transakcji płatniczej przez użytkownika, czy też mamy do czynienia z transakcją nieautoryzowaną, zależy odpowiedzialność zarówno dostawcy, jak i płatnika za transakcję płatniczą. Natomiast od ustalenia z jakich przyczyn doszło do wykonania nieautoryzowanej przez płatnika transakcji, zależy zakres odpowiedzialności dostawcy i obowiązku zwrotu kwot nieautoryzowanych transakcji.

W przypadku wystąpienia nieautoryzowanych przez płatnika transakcji płatniczych konieczne jest ustalenie, w jakich okolicznościach doszło do nieautoryzowanych transakcji: czy z winy płatnika wskutek naruszenia podstawowych obowiązków płatnika określonych w art. 42 ustawy o usługach płatniczych, czy też z powodu okoliczności, za które nie ponosi on odpowiedzialności, czy jednak z powodu okoliczności, za które ponosi odpowiedzialność dostawca. Od powyższych ustaleń uzależniona jest możliwość uzyskania przez płatnika zwrotu kwot nieautoryzowanych przez niego transakcji, zaś w wypadku niniejszej sprawy ustalenie kto ponosi za dokonane transakcje odpowiedzialność.

W art. 42 ustawy o usługach płatniczych wskazane zostały obowiązki użytkownika, które mają na celu zapewnienie minimum bezpieczeństwa transakcji płatniczych realizowanych z wykorzystaniem instrumentu płatniczego. Podstawowym obowiązkiem użytkownika jest więc korzystanie z instrumentu płatniczego zgodnie z postanowieniami umowy ramowej (jak również zgodnie z dołączonymi do umowy ramowej regulaminami, które stanowią integralną część umowy i określają zasady korzystania z instrumentu płatniczego – ust. 1 pkt 1). Kolejny obowiązek użytkownika – zgodnie z art. 42 ust. 1 pkt 2 – polega na powiadomieniu w przypadku utraty, kradzieży, przywłaszczenia czy też stwierdzenia, że doszło do nieuprawnionego skorzystania z instrumentu, dostawcy (lub podmiotu wskazanego w tym celu przez dostawcę) o zaistnieniu powyższego zdarzenia.

W przypadku powyższych roszczeń ciężar udowodnienia, że transakcja została autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Przypomnieć należy, że zgodnie z art. 6 k.c. ciężar udowodnienia faktu spoczywa na osobie, która z tego faktu wywodzi korzystane dla siebie skutki prawne. Ciężar udowodnienia, że transakcja była autoryzowana przez użytkownika, ciąży na dostawcy, nawet jeśli to użytkownik występuje z roszczeniem, twierdząc, że nie on autoryzował transakcji. Fakt zarejestrowanego użycia instrumentu płatniczego, czyli - należy przyjąć - użycia instrumentu płatniczego zgodnie z procedurami i przy zastosowaniu ustalonych sposobów autoryzacji, nie oznacza, że transakcja została autoryzowana przez użytkownika. W przypadku zgłoszenia przez użytkownika transakcji, które obciążają jego rachunek płatniczy i które były prawidłowo autoryzowane, czyli zlecone i zrealizowane zgodnie z przewidzianą procedurą, a które użytkownik wskazuje jako przez niego nieautoryzowane, dostawca musi udowodnić fakt autoryzacji transakcji przez użytkownika.

Przenosząc powyższe rozważania na grunt niniejszej sprawy wskazać należy, że dokonane przez powódkę transakcje, mimo iż zostały formalnie dokonane w sposób zgodny z przyjętymi przez bank procedurami, nie były faktycznie autoryzowane przez A. W.; powódka nie miała zamiaru i de facto świadomości wykonywanych transakcji w postaci przelewu kwoty 10.000 zł oraz transakcji z użyciem kodów BLIK w łącznej wysokości 10.000 zł.

Niemniej zachowanie powódki winno być oceniane w kontekście art. 46 ustawy o usługach płatniczych, w którym określono zasady odpowiedzialności dostawcy oraz płatnika w przypadku wystąpienia nieautoryzowanych transakcji. W myśl ust. 1 art. 46 ustawy o usługach płatniczych w przypadku wystąpienia nieautoryzowanych transakcji dostawca jest zobowiązany do niezwłocznego zwrotu płatnikowi kwoty nieautoryzowanej transakcji. Podstawowa zasada wskazuje więc obowiązek zwrotu przez dostawcę kwot nieautoryzowanych transakcji. Jeśli jednak do nieautoryzowanych transakcji płatnik doprowadził umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia swoich obowiązków (o których mowa w art. 42 ustawy o usługach płatniczych), wówczas odpowiada za wszystkie nieautoryzowane transakcje. O winie płatnika można mówić wówczas, gdy zaistniałe zdarzenie (czyli wystąpienie nieautoryzowanych transakcji) nastąpiło wskutek okoliczności, za które ponosi on odpowiedzialność.

W oparciu o zebrany materiał dowodowy Sąd Rejonowy ustalił, że powódka doprowadziła do uzyskania przez osoby trzecie dostępów do loginu, hasła, jak i kodów SMS, co umożliwiło im wyprowadzenie pieniędzy z rachunku powódki, skutkującego powstaniem debetu na rachunku o numerze (...) w wysokości 20.000 zł. Istotnym było przy tym ustalenie, czy w niedbalstwo po stronie powódki miało cechy rażącego niedbalstwa, jako kwalifikowanej formy winy czy cechy „zwykłego" niedbalstwa, o czym decydowało ustalenie wzorca staranności, wymaganego w stosunkach danego rodzaju.

Zgodnie z treścią art. 355 § 1 k.c. dłużnik obowiązany jest do staranności ogólnie wymaganej w stosunkach danego rodzaju (należyta staranność). Przez należytą staranność należy rozumieć staranność ogólnie wymaganą w stosunkach danego rodzaju. Jej wzorzec ma charakter obiektywny, a z kolei jego zastosowanie w praktyce polega najpierw na dokonaniu wyboru modelu ustalającego optymalny w danych warunkach sposób postępowania, odpowiednio skonkretyzowanego i aprobowanego społecznie, a następnie na porównaniu zachowania się dłużnika z takim wzorcem postępowania. O tym, czy na tle konkretnych okoliczności można osobie zobowiązanej postawić zarzut braku należytej staranności w dopełnianiu obowiązków, decyduje nie tylko niezgodność jej postępowania z modelem, lecz także uwarunkowana doświadczeniem życiowym możliwość i powinność przewidywania odpowiednich następstw zachowania. Miernik postępowania dłużnika, którego istotą jest zaniechanie dołożenia staranności, nie może być formułowany na poziomie obowiązków niedających się wyegzekwować, oderwanych od doświadczeń, reguł zawodowych, konkretnych okoliczności czy typu stosunków (wyrok SN z 17.05.2002 r., sygn. I CKN 1180/99, wyrok SN z 23.10.2003 r., sygn. V CK 311/02).

O stopniu niedbalstwa świadczy stopień staranności, jakiego w danych okolicznościach można wymagać od sprawcy. Niezachowanie podstawowych, elementarnych zasad ostrożności, które są oczywiste dla większości rozsądnie myślących ludzi, stanowi o niedbalstwie rażącym. Poziom elementarności i oczywistości wyznaczają okoliczności konkretnego stanu faktycznego, związane m.in. z osobą sprawcy, ale przede wszystkim zdarzenia obiektywne, w wyniku których powstała szkoda (wyrok SN z 10.08.2007 r., sygn. II CSK 170/07, wyrok SN z 10.03.2004 r., sygn. II CK 151/03).

Wskazać należy, że na powódce, jako osobie korzystającej z usług płatniczych w charakterze płatnika (art. 2 ust. 34 ustawy o usługach płatniczych) i uprawnionej do korzystania z instrumentu płatniczego, rozumianego jako zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywanych przez użytkownika do złożenia zlecenia płatniczego (art. 2 ust. 10 ustawy), spoczywał szereg obowiązków, sprowadzających się w istocie do korzystania z instrumentu płatniczego zgodnie z umową ramową, zgłaszania nieuprawnionego dostępu do instrumentu płatniczego oraz podejmowania środków odnośnie do zabezpieczenia instrumentu płatniczego i nieudostępniania go osobom nieuprawnionym.

W okolicznościach rozpoznawanej sprawy pierwszy z wymienionych wyżej obowiązków, tj. przestrzeganie umowy ramowej, sprowadzał się zaś w istocie do przyjętego w umowie obowiązku przestrzegania Regulaminu świadczenia usług (...) bankowości elektronicznej (...) Banku (...) S.A. co oznaczało z kolei obowiązek m.in. utrzymania w poufności wszystkich danych służących do jego identyfikacji i autoryzacji za pomocą systemu oraz nieujawniania tych danych osobom trzecim; zabezpieczenia używanych urządzeń elektronicznych, w tym mobilnych z zachowaniem należytej staranności tak, aby nie dopuścić do logowania do system osób trzecich (§ 36 Regulaminu); przestrzegania rekomendacji i zaleceń publikowanych przez Bank; upewniania się że środowisko komputerowe i środowisko urządzenia mobilnego jest bezpieczne (§ 35 ust. 2 i 3 Regulaminu).

Zdaniem sądu nieprzestrzeganie powyższych obowiązków przez powódkę jako płatnika (w rozumieniu ustawy), w tym sekwencja zdarzeń, do jakich doszło w dniu 17 września 2021 r. z udziałem powódki świadczy o jej rażącym niedbalstwie, co skutkowało – w świetle jednoznacznej regulacji przewidzianej w art. 46 ust. 3 ustawy – tym, że to właśnie powódka odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, co jednocześnie zwalnia z odpowiedzialności za te transakcje pozwany bank.

Na wstępie zwrócić należy uwagę, że powódka po odebraniu telefonu od osoby trzeciej nie dokonała żadnej weryfikacji tej osoby, a podającej się za pracownika banku. W ocenie sądu już w momencie pojawienia się ze strony rozmówcy polecenia instalacji na urządzeniu mobilnym powódki oprogramowania do obsługi pulpitu zdalnego AnyDesk, powódka winna wykazać się czujnością. Należy bowiem zwrócić uwagę, że w roku 2021, kiedy to doszło do zdarzenia z udziałem powódki, oszustwa internetowe i działania takie jak podszywanie się pod pracowników banku, zachęcenia do instalowania na telefonie niezweryfikowanych aplikacji, nie były zjawiskiem nowym, a wręcz stosowane przez oszustów praktyki były już powszechnie znane i wielokrotnie nagłaśniane w mediach, nadto pozwany bank ostrzegał swoich klientów w przystępny, a jednocześnie szczegółowy sposób. Powódka, zwłaszcza że jest osobą młoda, z wyższym wykształceniem ekonomicznym, winna zdawać sobie sprawę z płynących zagrożeń. Powódka powinna odmówić instalacji oprogramowania, a kolejno rozłączyć się i zadzwonić na numer infolinii banku celem weryfikacji zaistniałej sytuacji, czego jednak nie uczyniła.

Kolejnym sygnałem ostrzegawczym, który winien wzbudzić podejrzliwość powódki, winien być fakt, że po zalogowaniu się do bankowości elektronicznej powódka nie dostrzegła żadnych podejrzanych transakcji na swoim rachunku bankowym, subkont, mimo iż o takich transakcjach została poinformowana przez rozmówcę. Skoro bowiem osoba dzwoniąca (rzekomo) z banku twierdziła, że na rachunku bankowym powódki doszło do nieautoryzowanych transakcji, logicznym byłoby, że te transakcje były widoczne na rachunku bankowym powódki.

Niemniej w ocenie sądu najbardziej znamiennym przejawem rażącego niedbalstwa ze strony powódki, na co zwróciła uwagę również strona pozwana, był brak reakcji ze strony powódki na przychodzące wiadomości SMS, a zawierające kody autoryzacyjne operacji na rachunku powódki. Brak jakiejkolwiek refleksji na otrzymywane wiadomości SMS, w tym o treści: kod autoryzacyjny dla podpisania umowy kredytowej, robisz przelew na kwotę 10.000 zł, czy zmieniasz limity dla transakcji BLIK świadczą o braku rozwagi oraz lekkomyślności powódki. Podobnie w ocenie sądu niewiedzą czy manipulacją ze strony osoby trzeciej nie można usprawiedliwiać zachowania powódki przejawiającego się w odczytywaniu kodów BLIK a następnie potwierdzaniu dokonywanych za ich pomocą 10 transakcji BLIK w wysokości 1.000 zł każda, w swoim telefonie poufnym hasłem (...), co umożliwiło pobranie środków z rachunku powódki w bankomacie przez osoby trzecie.

Zwrócić również należy uwagę, że połączenie telefoniczne z osobą trzecią trwało, jak wskazała sama powódka około 1 godziny, zaś SMS-y przychodziły w odstępach kilku-kilkunastominutowych. Powódka wbrew jej twierdzeniom, miała zatem wystarczająco dużo czasu na zapoznanie się z treścią SMS-ów i zastanowienie się co te wiadomości faktycznie dla niej oznaczają.

Sąd zdaje sobie sprawę, że stosowane przez oszustów techniki mogą doprowadzić do manipulacji ofiary przestępstwa i podejmowania nieracjonalnych działań, niemniej w zaistniałym stanie faktycznym ilość sygnałów oraz czas w którym

można było podjąć jakąkolwiek reakcję przez powódkę przesądzają o rażącym niedbalstwie z jej strony. Nic bowiem w ocenie sądu nie usprawiedliwia braku jakiekolwiek czujności i reakcji na zaistniałe zdarzenie.

Reasumując, gdyby więc powódka dochowała choć minimalnej staranności i wykazała się odrobiną czujności przy posługiwaniu się systemem bankowości elektronicznej, nie udostępniłby przestępcom wszystkich danych potrzebnych do dokonania spornych transakcji.

Zdaniem Sądu Rejonowego, wbrew twierdzeniom powódki, nie doszło do złamania zabezpieczeń systemu bankowego. Powódka bowiem co wynika bezsprzecznie z ustalonego stanu faktycznego sama ujawniła osobom nieuprawnionym swoje poufne dane, a więc login, hasło, kody SMS, umożliwiając w ten sposób sprawcom przestępstwa ich przejęcie, a następnie wykorzystanie do dokonania transakcji. W tym zakresie strona pozwana zastosowała właściwe zabezpieczenia, ogólnie i powszechnie przyjęte w stosunkach tego rodzaju, a wyłudzenie danych nie wynikało z niesprawności systemów bankowych, czy nieszczelności stosowanych przez bank zabezpieczeń bądź niedochowania należytej staranności w sprawowaniu pieczy nad powierzonymi mu środkami finansowymi klientów.

W chwili zdarzenia, jak i przed zdarzeniem na stronie internetowe pozwanego banku widniały ostrzeżenia dotyczące zagrożeń w sieci. Jak wynikało z zebranego w sprawie materiału dowodowego – od października 2020 r. na stronach internetowych pozwanego banku publikowane były informacje o zagrożeniach w sieci; w tym komunikaty o tym, że oszuści dzwonią z numerów podszywających się pod infolinię banku. Ponadto bezpośrednio na skrzynkę mailową w bankowości elektronicznej należącą do powódki przychodziły powiadomienia o możliwych zagrożeniach. Powódka jednak jak sama wskazała, nie przywiązywała wagi do wymienionych komunikatów i nie zapoznawała się z nimi, mimo iż jak wynika z regulaminu usług stosowanego przez pozwany bank, jest to jednym z obowiązków każdego klienta banku.

Powódka zarzuciła, że takie transakcje jako nietypowe winny zostać zablokowane przez system bankowy. Z takim twierdzeniem sąd nie może się zgodzić: dobrodziejstwo bankowości elektronicznej polega – najogólniej rzecz ujmując – na możliwości dokonywania operacji bankowych w dowolnym momencie, wygodnie i szybko. Gdyby bank profilaktycznie blokował wszelkie odbiegające, nawet nieznacznie, od najczęściej wykonywanych transakcje i realizował je dopiero po upływie kilku-kilkunastu godzin, po skontaktowaniu się z klientem i uzyskaniu jego potwierdzenia, to w znaczący sposób ograniczyłoby to możność rozporządzania swoimi środkami; jednocześnie zwiększyłoby koszty działania banku (np. na wynagrodzenia pracowników, którzy dokonywaliby weryfikacji i ostatecznego zatwierdzenia operacji), co finalnie zwiększyłoby koszty ponoszone przez klientów. Należy przy tym zwrócić uwagę, że operacje wykonywane na rachunku powódki nie dotyczyły bardzo wysokich kwot: były to 10.000 zł i 1.000 zł. Choć kwota 10.000 zł stanowi około dwukrotność przeciętnego miesięcznego wynagrodzenia to niewątpliwie transakcje o takiej wartości są często dokonywane, np. opłata za zorganizowane wakacje dla 3-4-osobowej rodziny będzie częstokroć przekraczała tę kwotę, podobnie np. opłata za komplet mebli kuchennych. Wymienione operacje nie są oczywiście dokonywane codziennie, lecz są na tyle powszechne, że trudno sobie wręcz wyobrazić każdorazowe blokowanie takiej kwoty do czasu indywidualnego wyjaśnienia.

Podkreślenia wymaga, że korzystanie z bankowości elektronicznej jest możliwością, nie obowiązkiem klienta banku. Nadal osoba korzystająca z usług bankowych może wykonywać wszystkie czynności w oddziale, jak to działo się powszechnie kilkanaście lat temu, co wiązało się nie tylko z koniecznością wizyty w placówce w godzinach jej otwarcia, ale i z pokrywaniem opłat np. za przelewy (czego z reguły nie ma w bankowości elektronicznej) i – zazwyczaj – co najmniej kilkunastominutowym okresem oczekiwania w kolejce.

Konkludując w ocenie sądu roszczenie powódki w zakresie ustalenia, że powódka nie ponosi odpowiedzialności i nie jest zobowiązana do spłaty zobowiązań wynikających z nieautoryzowanych transakcji w łącznej kwocie 20.000 zł nie mogło zostać uwzględnione. Z tych samych przyczyn nie mogło zostać uwzględnione żądanie przywrócenia rachunku płatniczego do stanu jaki istniałby gdyby nie miały miejsca nieautoryzowane transakcje. W świetle powyższego orzeczono jak w punkcie II wyroku.

O kosztach procesu orzeczono w punkcie III wyroku w oparciu o przepis art. 100 zd. 1 k.p.c., zgodnie z którym w razie częściowego tylko uwzględnienia żądań koszty będą wzajemnie zniesione lub stosunkowo rozdzielone. W niniejszej sprawie dla rozliczenia kosztów przyjęto zaś, iż powódka wygrała sprawę w około 51 %.

W skład kosztów należnych powódce wchodziły: opłata sądowa od pozwu w kwocie 1.000 złotych, wynagrodzenie pełnomocnika w kwocie 3.600 złotych (§ 2 pkt 5 Rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności adwokackie - Dz. U. 2015.1800 ze zm.) oraz opłata od udzielonego pełnomocnictwa wynoszącą 17 złotych, co dało łączną sumę w wysokości 4.617 złotych, z czego 51% stanowi kwota 2.354,67 złotych.

W skład kosztów należnych stronie pozwanej, która wygrała sprawę w około 49%, wchodzą: wynagrodzenie pełnomocnika w kwocie 3.600 złotych oraz kwota 17 złotych tytułem opłaty za udzielenie pełnomocnictwa, co dało łączną sumę w wysokości 3.617 złotych, z czego 49 % stanowi kwota 1.772,33 zł.

Mając na względzie zatem wynik procesu, strona pozwana winna zwrócić powódce z tytułu kosztów procesu kwotę 582,34 zł (2.354,67-1.772,33) wraz z odsetkami ustawowymi za opóźnienie od dnia uprawomocnienia się orzeczenia do dnia zapłaty.