Sygnatura akt I C 1305/23/P

UZASADNIENIE

wyroku z dnia 20 grudnia 2023 roku

Powódka N. K. w pozwie z dnia 8 sierpnia 2023 r. skierowanym przeciwko Bankowi (...) S.A. z siedzibą w W. wniosła o zasądzenie na jej rzecz kwoty 9.700 zł tytułem zwrotu pieniędzy utraconych w wyniku nieautoryzowanych przez powódkę transakcji, z odsetkami ustawowymi za opóźnienie od dnia 22 września 2021 r. do dnia zapłaty. Powódka wniosła ponadto o zasądzenie kosztów procesu.

Na uzasadnienie podała, że strony łączy umowa rachunku bankowego nr (...). W dniu 16 września 2021 r. powódka otrzymała połączenie a na telefonie wyświetlił się numer infolinii Banku (...). Dzwoniący mężczyzna przedstawił się jako pracownik banku. Rozmówca znał dane powódki, w tym jej nazwisko. Poinformował powódkę, że jej konto zostało zablokowane z uwagi na podejrzane operacje jednakże trwają prace nad zabezpieczeniem środków i karty płatniczej powódki przed dalszymi nieuprawnionymi transakcjami. Dzwoniący zalecił powódce pobranie aplikacji (...), która miała na celu wychwytanie oszukańczych transakcji, jednak w rzeczywistości aplikacja ta umożliwia pracę na odległość pomiędzy różnymi urządzeniami oraz podgląd danych, o czym powódka wówczas nie wiedziała. Następnie dzwoniący przeprowadził powódkę przez cały proces instalacji aplikacji na jej telefonie. Jednocześnie poinformował ją, aby zignorowała wiadomości sms, które otrzyma albowiem dotyczą zablokowanych transakcji dokonywanych przez osoby trzecie, co też powódka uczyniła. Powódka była przekonana, że rozmawia z przedstawicielem pozwanego banku. Mężczyzna sprawiał wrażenie kompetentnego, używał profesjonalnego słownictwa. W czasie rozmowy powódka zalogowała się do bankowości internetowej i zauważyła, iż na jej rachunku pojawiły się nowe środki z tytułu pożyczki, o które nie wnioskowała. Powódka zorientowała się, że padła ofiarą oszustwa, rozłączyła się z rozmówcą i zadzwoniła na infolinię strony pozwanej.

Po rozmowie z pracownikiem banku okazało się, że dokonane zostały dwa przelewy wychodzące z rachunku powódki na kwotę 7000 zł i 2700 zł oraz znajdowało się uznanie w kwocie 14.911,26 zł z tytułu zawartej umowy pożyczki. Tego samego dnia powódka zgłosiła reklamację na wykonane transakcji jednakże strona pozwana odmówiła jej uznania argumentując, że wszystkie transakcje były prawidłowo autoryzowane. Powódka wskazała, że nie używała, nie zlecała oraz nie wpisywała żadnego kodu autoryzacyjnego zawartego w treści otrzymanych wiadomości sms skutkującego wyprowadzeniem środków z jej rachunku bankowego.

Powódka w dniu 20 września 2021 r. złożyła w banku reklamację za nieautoryzowane transakcje. Strona pozwana odmówiła uznania reklamacji. Nadto w dniu 17 września 2021 r. złożyła zawiadomienie o podejrzeniu popełnienia przestępstwa, wskutek czego zostało wszczęte dochodzenie w sprawie o sygn. RSD 1813/21, które ostatecznie zostało umorzone. Postanowieniem z dnia 16 sierpnia 2022 r. Sąd Rejonowy dla Krakowa-Podgórza w Krakowie utrzymał w mocy postanowienie o umorzeniu dochodzenia.

Jak dalej podnosi powódka, zapewnienie bezpieczeństwa depozytów jest jednym z najistotniejszych obowiązków banku. Tymczasem żadne mechanizmy ochronne systemu bankowego nie zareagowały na szereg nietypowych transakcji mających miejsce na rachunku bankowym powódki. Pozwany bank nie potwierdzał woli ani rzetelności tych transakcji, mając na względzie choćby ich ilość i częstotliwość, co powinno spowodować zablokowanie możliwości dokonania opisanych transakcji i uniemożliwienie ich realizacji. Po stronie pozwanej doszło zatem do uchybienia obowiązkom wynikającym z art. 50 ust. 2 Prawa bankowego (ochrona depozytów). Powódka domaga się zwrotu środków będących przedmiotem nieautoryzowanych i niewykonanych przez nią transakcji na podstawie art. 46 ustawy o usługach płatniczych.

Strona pozwana Bank (...) S.A. z siedzibą w W. w odpowiedzi na pozew z dnia 17 października 2023 r. wniosła o oddalenie powództwa w całości oraz o zasądzenie zwrotu kosztów postępowania.

Uzasadniając, strona pozwana zaprzeczyła, aby kwestionowała transakcja dokonana na rachunku bankowym powódki była nieuwierzytelniona, czy też nieautoryzowana. Powódka nie udowodniła okoliczności dotyczących spornej transakcji, w tym braku swojej zgody na jej dokonanie, bezprawnego działania osób trzecich, braku własnego przyczynienia się do utraty realizacji kwestionowanej transakcji. Strona pozwana wskazała na rażące niedbalstwo po stronie powódki w zakresie ochrony danych poufnych służących do korzystania z bankowości elektronicznej i posługiwanie się nimi w sposób lekkomyślny. Powódka nie wykazała również uchybień po stronie pozwanego banku w zakresie zapewnienie bezpieczeństwa zgromadzonych na rachunkach bankowych środkach.

Zdaniem strony pozwanej podnoszony przez powódkę zarzut braku autoryzacji należy uznać za bezzasadny. Wyłącznie bank – dostawca ma możliwość wykazania zewnętrznych przejawów autoryzacji transakcji tj. dokonania czynności wymaganych do zlecenia i akceptacji transakcji, ponieważ uwierzytelnianie stanowi procedurę stosowaną przez samego dostawcę. Skoro autoryzacja jest zgodą na dokonanie transakcji, to zgoda musi przybrać jakąś widoczną dla otoczenia formę. W przypadku transakcji płatniczych taką formę stanowi użycie instrumentu płatniczego, które to użycie jest poprzedzone uwierzytelnieniem. Samo twierdzenie klienta, że transakcja nie była autoryzowana, nie stanowi obowiązku uznania, iż tak rzeczywiście było.

Co więcej, obowiązek przywrócenia rachunku do stanu sprzed nieautoryzowanej transakcji nie wyłączony w warunkach z art. 46 ust. 3 ustawy o usługach płatniczych tj. gdy płatnik doprowadził do nieautoryzowanej transakcji umyślnie albo gdy transakcja jest wynikiem rażącego niedbalstwa i naruszenia co najmniej jednego z obowiązków określonych w art. 42 ww. ustawy. Przepis art. 46 ustawy o usługach płatniczych nie może być stosowany w sposób prowadzący do nieuzasadnionego wzbogacenia płatnika. Jeśli dostawca dysponuje dostatecznymi dowodami, że płatnik ponosi odpowiedzialność za transakcję nieautoryzowaną albo wyraził zgodę na jej wykonanie, dostawca nie jest zobowiązany, aby w tym zakresie przekazać płatnikowi środki pieniężne.

Powódka była wielokrotnie informowana o metodach działania przestępców oraz zasadach bezpiecznego korzystania z systemów transakcyjnych banku. Do powódki były kierowane (m.in. w ramach systemu aplikacji mobilnej M.) wielokrotne komunikaty o bezpieczeństwie. Zdaniem pozwanego banku zachowanie powódki nosiło cechy rażącego niedbalstwa.

Jak dalej zauważa pozwany bank, wysokość kwoty kwestionowanej transakcji nie odbiegała znacząco od transakcji dokonywanych przez powódkę przed datą przedmiotowej transakcji. Nie było zatem podstaw, aby transakcja przelewu z 16 września 2021 r. miała wzbudzić podejrzenia banku i stanowić podstawę do zastosowania szczególnych procedur bezpieczeństwa.

Strona pozwana zakwestionowała również żądanie o zapłatę odsetek ustawowych, wskazując iż termin do zapłaty został określony wadliwie.

Sąd ustalił, następujący stan faktyczny:

Strony łączy umowa rachunku DOBRE KONTO zawarta 6 lipca 2011 r. w K.. Na mocy umowy pozwany bank zobowiązał się do prowadzenia rachunku oszczędnościowo-rozliczeniowego w PLN o numerze (...). Dodatkowo powódka zawarła umowę konta oszczędnościowego (...). W dniu 7 marca 2012 r. strony zawarły umowę ramową o świadczenie usług finansowych, uprawniającą do korzystania z usług finansowych w Banku (...) S.A. W sprawach nieuregulowanych w umowie strony związane były Regulaminem.

Zgodnie z § 29 ust. 1 Regulaminu zlecenie przelewu stanowi udzieloną Bankowi przez posiadacza rachunku instrukcję obciążenia jego rachunku bankowego i uznania tą kwotą rachunku Odbiorcy. Zlecenie przelewu może zostać złożone za pośrednictwem K. (Kanału B.) lub w placówce Banku (§ 29 ust. 1 Regulaminu). Dostarczenie do Banku prawidłowego zlecenia przelewu oznacza zgodę Posiadacza rachunku na jego wykonanie (§ 29 ust. 6 Regulaminu).

Bank przekazuje Użytkownikowi K. M. (§ 58 ust. 1 Regulaminu). Do aktywacji K. w zakresie Usług bankowości elektronicznej lub Usługi bankowości telefonicznej wymagane jest: 1) podanie HasłaSMS lub odebranie połączenia

wykonanego na zdefiniowany numer telefonu i poprawne wykonanie czynności podanych przez Bank oraz 2) podanie Hasła tymczasowego (§ 58 ust. 2 Regulaminu). Aktywacja Aplikacji mobilnej na urządzeniu jest równoznaczna z przypisaniem do użytkownika K. Zaufanego Urządzenia (§ 58 ust. 3 Regulaminu). Każdorazowy dostęp do K. przy Użytkownika K. możliwy jest po podaniu Danych identyfikujących (§ 58 ust. 4 Regulaminu).

Zdefiniowany numer telefonu komórkowego, na który wysyłane są Hasła SMS, staje się numerem do kontaktu z Użytkownikiem K. (§ 62 ust. 2 Regulaminu). Użytkownik K. powinien posługiwać się Danymi identyfikującymi, dokonywać Autoryzacji oświadczenia oraz posługiwać się elementami, o których mowa w § 17 ust. 7 w sposób zapewniający zachowanie ich poufności, w szczególności zobowiązany jest do nieudostępniania ich osobom nieupoważnionym (§ 62 ust. 7 Regulaminu).

Zgodnie z § 17 ust. 7 Regulaminu lista elementów uwierzytelnienia, z których Użytkownik K. lub Posiadacz karty może korzystać (w zależności od komunikatu podanego przez Bank) obejmuje: Autoryzację mobilną, Bezpieczną kopertę, Dane aktywowane z użyciem modułu biometrycznego, H@sło1, Hasło mobilne, Kartę płatniczą, (...), (...) mobilny, Zaufaną przeglądarkę, Zaufane urządzenie, Zdefiniowany numer telefonu.

Korzystanie z K. jest możliwe pod warunkiem użycia sprzętu skonfigurowanego zgodnie z zaleceniami Banku oraz oprogramowania udostępnionego lub rekomendowanego przez Bank. Zalecenia Banku określone są na stronie internetowej Banku, z P. Banku oraz za pośrednictwem (...) (§ 65 ust. 1 Regulaminu). Użytkownik K. korzystający z systemu M. jest zobowiązany do monitorowania serwisu internetowego Banku, w celu aktualizacji wiedzy na temat obsługi M. oraz wymagań sprzętowych i programowych (§ 65 ust. 3 Regulaminu). Użytkownik K. zobowiązany jest do przestrzegania zasad bezpieczeństwa przy korzystaniu z K., umieszczonych na stronie internetowej Banku (§ 65 ust. 4 Regulaminu). Użytkownik K. powinien zwracać szczególną uwagę na niestandardowe komunikaty o konieczności przeprowadzenia dodatkowych instalacji na Urządzeniu mobilnym lub komputerze (§ 65 ust. 5 Regulaminu).

Korzystanie przez Użytkownika BLIK z płatności mobilnych BLIK na danych urządzeniu mobilnym możliwe jest, jeśli użytkownik BLIK ma aktywny dostęp do aplikacji mobilnej (§ 72 ust. 2 Regulaminu).

Posiadacz rachunku korzystający z Aplikacji mobilnej w tym płatności mobilnych BLIK zobowiązany jest do: 1. Zabezpieczenia urządzenia mobilnego wraz z zainstalowaną Aplikacją Mobilną oraz do przestrzegania zasad bezpieczeństwa przy jej korzystaniu, umieszczonych na stronie internetowej banku, 2. Niezwłocznego zgłoszenia do Banku w przypadku utraty, kradzieży, przewłaszczenia urządzenia mobilnego lub nieuprawnionego korzystania z Aplikacji Mobilnej, 3. Nieudostępniania osobom trzecim narzędzi służących do weryfikacji i uwierzytelniania w Aplikacji Mobilnej (§ 76 ust. 1 Regulaminu).

Użytkownika BLIK obciążają płatności mobilne BLIK dokonane za pośrednictwem Aplikacji Mobilnej przez osoby, którym ujawnił (...) mobilny (§ 76 ust. 2 Regulaminu). Użytkownika BLIK obciążają płatności mobilne BLIK dokonane czekiem BLIK przez osoby trzecie, którym udostępnił hasło do czeku BLIK (§ 76 ust. 3 Regulaminu). Użytkownik BLIK odpowiada za nieautoryzowane transakcje, jeśli doprowadził do nich umyślnie lub w wyniku umyślnego albo będącego skutkiem rażącego niedbalstwa naruszenia jednego z obowiązków, o których mowa w ust. 1 pkt 1-3 (§ 76 ust. 4 Regulaminu). Użytkownik BLIK odpowiada za nieautoryzowane Płatności Mobilne BLIK 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 ust. 1 (§ 76 ust. 8 Regulaminu).

Zgodnie z § 40 ust. 1 Regulaminu karta debetowa umożliwia dokonywanie transakcji kartą debetową, a także składanie innych dyspozycji. Transakcje bezgotówkowe mogą być dokonane również na odległość – bez fizycznego przedstawienia karty, przez Internet, telefonicznie lub za pośrednictwem poczty (§ 40 ust. 3 Regulaminu).

Przy transakcjach Kartą debetową dokonanych na odległość bez fizycznego jej przedstawienia Posiadacz karty może zostać poproszony w celu Autoryzacji o podanie Unikatowego identyfikatora, daty ważności, imienia i nazwiska oraz dodatkowego kodu (...), widniejącego na odwrocie karty (§ 40 ust. 7 Regulaminu).

W przypadku transakcji, o których mowa w ust. 7, Posiadacz karty może zostać poproszony o podanie dodatkowego elementu zabezpieczającego w ramach usługi 3D S.. Usługa 3D S. jest rozumiana jako metoda uwierzytelniania bezgotówkowej Transakcji kartą debetową przez Internet (§ 40 ust. 8 Regulaminu).

Dowód: umowa rachunku oszczędnościowo-rozliczeniowego (k. 81-82), umowa konta oszczędnościowego (k. 19), umowa ramowa o świadczenie usług finansowych (k. 17), Regulamin (k. 83-92)

Powódka w dniu 16 września 2021 r. otrzymała połączenie telefoniczne, które odebrała. Rozmówca przedstawił się jako osoba z ochrony banku (...) S.A. i poinformował, że na jej rachunku bankowym miała miejsce próba włamania. Powódka odpowiedziała dzwoniącemu, że z Bankiem (...) nie ma nic wspólnego i odłożyła słuchawkę.

Chwilę później powódka otrzymała kolejne połączenie jednak tym razem na telefonie wyświetliła się infolinia pozwanego banku. Rozmówca przedstawił się jako osoba z ochrony banku (...) i zapytał czy rozmawia z N. K., co też powódka potwierdziła. Poinformował powódkę, że na jej koncie miała miejsce próba kradzieży i należy zabezpieczyć jej konto i kartę w czym jej pomoże jednak najpierw musi na swój telefon ściągnąć aplikację (...). Prowadził rozmowę w sposób profesjonalny. Powódka nie sprawdziła do czego służy aplikacja. Mężczyzna poprowadził powódkę przez proces jej instalacji. Po zainstalowaniu aplikacji dzwoniący powiedział powódce, że na jej telefon będą przychodzić smsy dotyczące kwoty jaką próbowali przejąć złodzieje. Prosił by je zignorowała, co też powódka uczyniła. Powódka na prośbę mężczyzny skopiowała jednego z smsów i próbowała dalej przesłać do niego, jednak bezskutecznie. Wówczas mężczyzna poprosił o podanie mu kwoty, którą była w treści wiadomości. Powódka smsem przesłała mu tę kwotę.

Następnie poinformował powódkę, że na jej dane została podjęta próba zaciągnięcia kredytu w kwocie 15.000 zł i należy znowu zabezpieczyć ten kredyt. Powódka wówczas nabrała podejrzeń i rozłączyła się, po czym zalogowała się przez telefon komórkowy wpisując swój login i hasło na konto bankowe. Zauważyła, iż na jej koncie brak był środków oraz widnieje zaciągnięta pożyczka. W tym momencie mężczyzna ponownie zadzwonił do powódki z propozycją zabezpieczenia kredytu. Powódka poinformowała go, iż ma świadomość, że została okradziona i będzie kontaktować się z infolinią banku.

Po skontaktowaniu się z infolinią Banku, powódka otrzymała informację, że wszystko transakcje zostały przez nią autoryzowane. Ponadto została poproszona o przywrócenie telefonu do ustawień fabrycznych, co też uczyniła.

W czasie rozmowy z powódka nie podała swoich danych ani loginu do rachunku bankowego. Powódka podała dzwoniącemu wybrane cyfry z jej numeru PESEL. N. K. działała pod wpływem stresu i z obawy przed ewentualną kradzieżą jej środków.

Dowód: zeznania powódki (k. 130-131), płyta CD (k. 56)

Pozwany bank wielokrotnie w M. i w aplikacji mobilnej informował powódkę o zasadach bezpiecznego korzystania z bankowości elektronicznej oraz stosowanych przez oszustów metodach wyłudzania danych, w tym instalowaniu podejrzanych aplikacji m.in. w komunikatach przesłanych w dniach: 19.05.2020 r., 21.07.2020 r., 24.09.2020 r., 9.10.2020 r., 7.12.2020 r., 2.03.2021 r., 9.04.2021 r., 13.05.2021 r., 21.05.2021 r., 11.06.2021 r., 8.07.2021 r., 14.07.2021 r., 29.07.2021 r., 20.08.2021 r., 26.08.2021 r. Powódka nigdy nie zapoznawała się z treścią przesłanych komunikatów.

Dowód : komunikaty bezpieczeństwa banku (k. 95), zeznania powódki (k. 130-131),

Suma wyprowadzonych z konta powódki środków wyniosła 9.700 zł. Jednocześnie na rachunku znajdowało się uznanie na kwotę 14.911,26 zł z tytułu zawartej umowy pożyczki.

Dowód: zestawienie transakcji od 1.09.2021 r. do 30.09.2021 r. (k. 21)

W dniu 20 września 2021 r. powódka złożyła w banku reklamację na nieautoryzowane transakcje. Pozwany bank w piśmie z dnia 7 października 2021 r. oraz z dnia 19 kwietnia 2022 r. odmówił uznania reklamacji.

Dowód: reklamacja (k. 23), odpowiedzi na reklamację (k. 25-29)

W dniu 20 września 2021 r., na skutek złożonego przez powódkę zawiadomienia, zostało wszczęte dochodzenie o sygn. RSD 1913/21, m.in. w sprawie zaistniałego w dniu 16 września 2021 r. w nieustalonym miejscu ze skutkiem w K., wpływania bez upoważnienia, w celu osiągnięcia korzyści majątkowej na automatyczne przetwarzanie danych informatycznych zgromadzonych na serwerach Banku (...) S.A. i wykonania za pośrednictwem rachunku bankowego zarejestrowanego na dane N. K. nieautoryzowanych transakcji na łączną kwotę 9.700 zł. Dochodzenie zostało umorzone z uwagi na niewykrycie sprawcy. Postanowieniem z dnia 16 sierpnia 2022 r. Sąd Rejonowy dla Krakowa-Podgórza w Krakowie, II Wydział Karny utrzymał w mocy zaskarżone postanowienie o umorzeniu.

Dowód: potwierdzenie złożenia zawiadomienia (k.22), zawiadomienie o wszczęciu dochodzenia (k. 8 akt sprawy o sygn. RSD 1913/21), postanowienie o umorzeniu dochodzenia (k. 14-16 akt sprawy o sygn. II Kp 490/22/P).

Stan faktyczny Sąd ustalił na podstawie załączonych przez strony do akt sprawy dokumentów, których moc dowodowa nie była kwestionowana. Sąd uznał je za wiarygodne w całości.

Dokumentacja zgromadzona w aktach sprawy jest w pełni wiarygodna, dlatego Sąd czynił ustalenia faktyczne w oparciu o takie dokumenty jak: umowa rachunku oszczędnościowo-rozliczeniowego, umowa konta oszczędnościowego, umowa ramowa o świadczenie usług finansowych, Regulamin, zestawienie transakcji od 1.09.2021 r. do 30.09.2021 r., komunikaty bezpieczeństwa banku, reklamacja, odpowiedzi na reklamację, potwierdzenie złożenia zawiadomienia, zawiadomienie o wszczęciu dochodzenia, postanowienie o umorzeniu dochodzenia. Autentyczność tych dokumentów nie była kwestionowana przez żadną ze stron i nie budziła żadnych wątpliwości Sądu.

Zgodnie z wiążącymi strony umowami pozwany w ramach usług bankowości elektronicznej zobowiązany jest do stosowania szeregu procedur, mających chronić klientów przed oszustwami. Bank wykazał, że procedur tych przestrzega, a stosowane przez niego standardy – zwłaszcza w zakresie autoryzacji transakcji przez dysponenta konta – są wysokie.

Sąd ustalił stan faktyczny również w oparciu o zeznania powódki – zwłaszcza odnośnie jej interakcji z oszustem, którego padła ofiarą. Jej relacje Sąd uznał za zasługujące na wiarę, logiczne i spójne, jako że pokrywały się z pozostałym materiałem dowodowym zgromadzonym w sprawie. Jakkolwiek na skutek manipulacji pozostała ona w błędzie co do charakteru dokonywanych czynności, to jednak nie budzi wątpliwości, że bezrefleksyjnie przekazała osobie trzeciej wszystkie dane bankowości elektronicznej niezbędne do autoryzacji, a następnie przeprowadzenia kwestionowanych transakcji. Powyższe wynika wprost z treści jej zeznań i potwierdzone zostało również nagraniem zgłoszenia zdarzenia załączonym do odpowiedzi na pozew na płycie CD.

Pozostałe dokumenty przedłożone przez strony nie przyczyniły się do rozpoznania niniejszej sprawy.

Sąd zważył, co następuje:

Sąd podzielił stanowisko strony pozwanej co do okoliczności, że po stronie powodowej doszło do rażącego niedbalstwa, co musiało skutkować oddaleniem powództwa w niniejszej sprawie.

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

Jak stanowi art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2021 r. poz. 2439 z późn. zm.) bank dokłada szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych.

Zastosowanie w sprawie znalazła także ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2021 r. poz. 1907 z późn. zm.), określająca zasady świadczenia usług płatniczych oraz wydawania i wykupu pieniądza elektronicznego. Bez wątpienia w przedmiotowej sprawie dochodziło do realizowania przez dostawcę usług płatniczych, wymienionych w art. 3 ustawy. Stosował on przy tym procedury uwierzytelniające, definiowane w art. 2 ustawy (pkt 33 b) jako procedury umożliwiające dostawcy usług płatniczych weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających.

Obowiązki dostawcy wydającego instrument płatniczy reguluje art. 43 u.u.p, wskazując, iż jest on obowiązany do:

1) zapewnienia, że indywidualne dane uwierzytelniające nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu,

2) niewysyłania niezamówionego instrumentu płatniczego, z wyjątkiem sytuacji, w których instrument płatniczy otrzymany przez użytkownika podlega wymianie,

3) zapewnienia stałej dostępności odpowiednich środków pozwalających użytkownikowi na dokonanie zgłoszenia zgodnie z art. 42 ust. 1 pkt 2 lub wystąpienie z wnioskiem o odblokowanie albo zastąpienie zablokowanego instrumentu płatniczego nowym na podstawie art. 41 ust. 4,

4) zapewnienia procedur pozwalających na udowodnienie dokonania zgłoszenia, o którym mowa w art. 42 ust. 1 pkt 2, na wniosek złożony przez użytkownika w terminie 18 miesięcy od dnia dokonania zgłoszenia,

5) zapewnienia użytkownikowi możliwości bezpłatnego dokonania zgłoszenia, zgodnie z art. 42 ust. 1 pkt 2, oraz nienakładania opłat w wysokości przekraczającej koszty bezpośrednio związane z wydaniem nowego instrumentu płatniczego w miejsce instrumentu, którego zgłoszenie dotyczy, oraz

6) uniemożliwienia korzystania z instrumentu płatniczego po dokonaniu zgłoszenia zgodnie z art. 42 ust. 1 pkt 2.

Jednocześnie dostawca ponosi ryzyko związane z wysłaniem płatnikowi instrumentu płatniczego lub indywidualnych danych uwierzytelniających (ust. 2 ww. art.).

Ciężar udowodnienia autoryzacji transakcji przez użytkownika wynika z art. 45 u.u.p., zgodnie z którym na dostawcy użytkownika spoczywa ciężar udowodnienia, że transakcja płatnicza została autoryzowana i prawidłowo zapisana w systemie służącym do obsługi transakcji płatniczych dostawcy oraz że nie miała na nią wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą świadczoną przez tego dostawcę, w tym dostawcę świadczącego usługę inicjowania transakcji płatniczej (ust. 1). Jednocześnie wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana albo że płatnik umyślnie albo wskutek rażącego niedbalstwa doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie albo wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42. Ciężar udowodnienia tych okoliczności spoczywa na dostawcy (ust. 2).

Zgodnie z art. 46 ust. 1 u.u.p. z zastrzeżeniem art. 44 ust. 2, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika niezwłocznie, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwraca płatnikowi kwotę nieautoryzowanej transakcji płatniczej, z wyjątkiem przypadku gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw. W przypadku gdy płatnik korzysta

z rachunku płatniczego, dostawca płatnika przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. Data waluty w odniesieniu do uznania rachunku płatniczego płatnika nie może być późniejsza od daty obciążenia tą kwotą.

Jak wskazuje art. 46 ust. 3 u.u.p. 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, który stanowi w ust. 1, iż użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany korzystać z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. W celu spełnienia obowiązku, o którym mowa w ust. 1 pkt 1, użytkownik, z chwilą otrzymania instrumentu płatniczego, podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (ust. 2 przepisu). Jednocześnie umowa ramowa, o której mowa w ust. 1 pkt 1, powinna zawierać obiektywne, niedyskryminujące i proporcjonalne postanowienia dotyczące wydawania i użytkowania instrumentu płatniczego (ust. 3).

Biorąc pod uwagę ustalony stan faktyczny przedmiotowej sprawy oraz przytoczone powyżej uregulowania, nie można zgodzić się z twierdzeniem powódki jakoby nie sposób było przypisać jej umyślności czy rażącego niedbalstwa, o których mowa w art. 46 ust. 3 ustawy o usługach płatniczych. W ocenie Sądu pozwany bank wykazał nie tylko samo zarejestrowane użycie instrumentu płatniczego, ale przede wszystkim rażące niedbalstwo powódki, skutkujące naruszeniem przez nich co najmniej jednego z obowiązków, o których mowa w art. 42 (zwłaszcza wskazanych w ust. 2). Tym samym zgodnie z art. 46 ust. 3 u.u.p. to powódka jako płatnik odpowiada za zaistniałe nieautoryzowane transakcje płatnicze w pełnej wysokości. Z uwagi na powyższe, powództwo nie zasługiwało na uwzględnienie.

Pozwany bank udowodnił, że wywiązał się z wypełnienia swoich ustawowych obowiązków dostawcy wydającego instrument płatniczy, wskazanych w art. 43 u.u.p, m.in. zapewniając, że indywidualne dane uwierzytelniające nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu.

Użytkownik uprawniony do korzystania z instrumentu płatniczego również ma pewne obowiązki, w tym korzystania z instrumentu płatniczego zgodnie z umową ramową. W celu spełnienia tego obowiązku użytkownik jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (art. 42 ust. 1 pkt 1 i ust. 2 u.u.p). Zgodnie z § 65 ust. 5 Regulaminu łączącego strony Użytkownik K. powinien zwracać szczególną uwagę na niestandardowe komunikaty o konieczności przeprowadzenia dodatkowych instalacji na Urządzeniu mobilnym lub komputerze. Natomiast stosowanie do § 76 ust. 1 Regulaminu posiadacz rachunku korzystający z Aplikacji mobilnej w tym płatności mobilnych BLIK zobowiązany jest w szczególności do nieudostępniania osobom trzecim narzędzi służących do weryfikacji i uwierzytelniania w Aplikacji Mobilnej.

W celu spełnienia obowiązków, o którym mowa w art. 42 u.u.p powódka powinna była podjąć niezbędne środki służące zapobieżeniu naruszeniu indywidualnych danych uwierzytelniających, w szczególności obowiązana była do nieudostępniania go osobom nieuprawnionym. W świetle dokonanych ustaleń, nie ulega wątpliwości, że powódka samodzielnie dokonała zainstalowania na swoim telefonie aplikacji służącej do bieżącego monitorowania jej aktywności w czasie rzeczywistym, w tym śledzenia wpisywanych danych i haseł. Następnie przesyłała swojemu rozmówcy dane służące do autoryzacji poszczególnych transakcji, tj. wszystkie hasła sms niezbędne do zrealizowania operacji, które inicjowała nieuprawniona osoba. Hasła autoryzacyjne bank wysyłał na numer telefonu powódki – zgodnie z łączącą strony umową. To powódka doprowadziła do tego, że osoba trzecia uzyskała dane pozwalające jej na wyprowadzenie środków z jej konta. Skoro do ujawnienia danych uwierzytelniających i autoryzacyjnych doszło świadomie i z winy użytkownika to bank nie ponosi odpowiedzialności za straty jego środków finansowych.

Istotnym było ustalenie, czy niedbalstwo powódki miało cechy rażącego niedbalstwa, jako kwalifikowanej formy winy, o czym decydowało ustalenie wzorca staranności, wymaganego w stosunkach danego rodzaju. Jak stanowi art. 355 §

1 k.c. dłużnik obowiązany jest do staranności ogólnie wymaganej w stosunkach danego rodzaju (należyta staranność). 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 (zob. wyroki SN z dnia 17 maja 2002 r., I CKN 1180/99; z dnia 23 października 2003 r., V CK 311/02; z dnia 8 lipca 1998 r., III CKN 574/97). Pojęcie należytej staranności jest miernikiem, który służy do ustalenia winy w postaci niedbalstwa, gdy stanowi ona przesłankę zastosowania określonego przepisu (wyrok Sądu Najwyższego z dnia 30 marca 2000 r. sygn. akt III CKN 709/98). 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 Sądu Najwyższego z dnia 10 sierpnia 2007 r., sygn. akt II CSK 170/07, por. też wyrok Sądu Najwyższego z dnia 10 marca 2004 r., sygn. akt IY CK 151/03).

W ocenie Sądu niedbalstwo, jakiego dopuściła się powódka miało charakter rażący. Polegało na braku zachowania wymaganej staranności w czynnościach bankowych. Powódka bezrefleksyjnie przekazała osobie nieuprawnionej poufne dane autoryzacyjne, naruszając tym samym zarówno postanowienia łączących ją ze stroną pozwaną umów, jak również obowiązki płatnika wskazane w ustawie o usługach płatniczych. Powódka nie dochowała minimum środków bezpieczeństwa. W przedmiotowej sprawie pozwany bank wyczerpał wszelkie możliwości uchronienia powódki przed przestępstwem, jakiego padła ofiarą. Fakt, iż podjęte przez niego działania okazały się nieskuteczne jest wyłącznie efektem nieodpowiedzialnego postępowania klienta, który naruszył zasady bezpiecznego korzystania z bankowości elektronicznej. Ustalenia poczynione w tym zakresie potwierdziła sama powódka w swoich zeznaniach. Jak sama przyznała, nie czytała komunikatów dotyczących bezpieczeństwa wysyłanych przez bank. Bezrefleksyjnie ściągnęła aplikację na swój telefon nie czytając jej opisu i nie sprawdzając do czego w istocie służy. Dzięki aplikacji sprawca uzyskał dostęp do danych powódki umożliwiających zalogowanie się bankowości internetowej. Co więcej, przesyłała osobie nieuprawnionej wiadomości sms zawierające dane uwierzytelniające do dokonanych transakcji. Na uwagę zasługuje również, iż osoba podszywająca się pod bank wskazała w pierwszej kolejności, że chodzi o włamanie na konto powódki w banku (...). Jednakże powódka zignorowała tę „pomyłkę" informując, że nie posiada we wspomnianym banku konta. Nawet taka okoliczność nie spowodowała jej wzmożonej czujności.

W oparciu o zgromadzony w sprawie materiał dowodowy Sąd ustalił, że to powódka dopuściła się rażącego niedbalstwa przez niezachowanie podstawowych zasad bezpieczeństwa wobec czego nie sposób przypisać stronie pozwanej niewłaściwego wykonywania łączącej strony umowy.

Z uwagi na powyższe, Sąd orzekł jak w punkcie I wyroku.

O kosztach postępowania Sąd orzekł na podstawie art. 98 § 1 i 3 k.p.c., zgodnie z którym strona przegrywająca spraw obowiązana jest zwrócić przeciwnikowi na jego żądanie koszty niezbędne do celowego dochodzenia praw i celowej obrony (koszty procesu). Na koszty te złożyło się wynagrodzenie profesjonalnego pełnomocnika w kwocie 1.800 zł ustalone na podstawie § 2 pkt 4 Rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności adwokackie oraz 17 zł tytułem opłaty skarbowej od pełnomocnictwa. O odsetkach zasądzonych od kwoty kosztów orzeczono na podstawie art. 98 § 1^1 k.p.c.