Sygn. akt I C 926/20

UZASADNIENIE

wyroku z 26 kwietnia 2021 r.

Pozwem z 10 października 2020 roku ***powód A. B. (1)*** wniósł o zasądzenie na jego rzecz od ***strony pozwanej Banku (...) spółki akcyjnej z siedzibą w W.*** kwoty 25.000 zł wraz z odsetkami ustawowymi za opóźnienie liczonymi od 1 lipca 2020 r. do dnia zapłaty. Nadto wniósł o zasądzenie na jego rzecz kosztów procesu.

Dla uzasadnienia swojego pozwu podał, iż 4 maja 2020 r. na skutek dokonanych przez osoby trzecie transakcji płatniczych, które nie zostały przez powoda osobiście autoryzowane, z należących do niego rachunków bankowych, wyprowadzona została kwota w łącznej wysokości 25.000 zł. Powód podjął szybkie i niezbędne działania, które zapobiegły dalszym kradzieżom (zgłoszenie nieautoryzowanych transakcji, wyłączenie karty SIM, zgłoszenie sprawy organom ścigania). Dochował w ten sposób należytej staranności. Bank winien zwrócić na jego rzecz kwoty wytransferowane przez nieautoryzowane transakcje płatnicze. Bank ponosi w tym zakresie odpowiedzialność na zasadzie ryzyka.

Strona pozwana, w sprzeciwi od wydanego nakazu zapłaty, wniosła o oddalenie powództwa, a także o zasądzenie od powoda na jej rzecz kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych. Strona pozwana podniosła przeciwko żądaniu pozwu zarzut braku legitymacji biernej.

W uzasadnieniu swojego sprzeciwu strona pozwana podała, iż wszystkie sporne transakcje płatnicze zostały potwierdzone przez kod sms, który powód otrzymał każdorazowo na swój numer telefonu komórkowego. Bank otrzymał prawidłowe – zgodne z obowiązującymi procedurami wewnątrzbankowymi – dyspozycje aktywacji aplikacji, realizacji przelewów oraz wypłat BLIK i był zobowiązany je wykonać. Bank nie ponosi odpowiedzialności za prawidłowo zrealizowane transakcje dokonane przed otrzymaniem dyspozycji blokady Kanałów B.. Powód w żaden sposób nie udowodnił braku winy.

Sąd ustalił następujący stan faktyczny.

16 września 2008 r. A. B. (1) zawarł z Bankiem (...) spółką akcyjną z siedzibą w W. umowę rachunku oszczędnościowo-rozliczeniowego oraz innych rachunków bankowych. Zostały mu przypisane następuje numery rachunków bankowych: (...) oraz (...) (...) (...).

A. B. (1) korzystał z usług oferowanych przez Bank za pośrednictwem Kanałów B. (w tym płatności BLIK). Czynności bankowe dokonywane w ramach bankowości elektronicznej dokonywał z własnego komputera bądź za pośrednictwem aplikacji w telefonie.

A. B. (1) uzyskał osobisty M. (ośmiocyfrowy) oraz osobiste hasło 1 (ośmiocyfrowe), które służyły do identyfikacji posiadacza rachunku oraz umożliwiały dostęp do kanałów B. (§46 ust. 1 pkt 2 Regulaminu). Logowanie od rachunku odbywało się przy użyciu millekodu, który jest przypisany do rachunku. Kod ten jest kodem indywidualnym i przypisanym do posiadacza rachunku. Posiadacz rachunku nie miał możliwości zmiany tego kodu. KOljnym etapem logowania do rachunku za pośrednictwem internetu było wprowadzenie hasła. Potwierdzenie zaś dokonanych czynności na rachunku za pośrednictwem bankowości elektronicznej obywało się przez bądź poprzez wpisanie kodu nadesłanego za pośrednictwem SMS lub poprzez wpisanie w aplikacji czterocyfrowego kodu. Jeżeli zaś operacje były dokonywane za pośrednictwem aplikacji w telefonie nie było wymagane podawanie millekodu i hasła, a jedynie podanie tych danych było konieczne przy zainstalowaniu aplikacji. Przy kolejnych czynnościach wymagane było podawanie czterocyfrowego pinkodu, Aplikacja rozpoznaje model telefonu, na którym została zainstalowana.

Zgodnie § 46 ust. 2 Regulaminu (...) Świadczenia Usług (...) dla Osób Fizycznych w Banku (...), obowiązującego w dacie podpisania umowy rachunku oszczędnościowo-rozliczeniowego oraz innych rachunków bankowych, posiadacz

rachunku może otrzymywać z Banku na zdefiniowany w M. (system komunikacji internetowej) numer telefonu komórkowego jednorazowe hasła sms służące do autoryzacji wybranej dyspozycji, dla której hasło sms zostało wygenerowane.

Posiadacz rachunku powinien niezwłocznie dokonać w Kanałach B. blokady numeru telefonu komórkowego, o którym mowa w ust. 2, w przypadku jego zgubienia, zmiany lub kradzieży (§ 46 ust. 9 Regulaminu).

Zgodnie z postanowieniami zawartymi w § 51 ust. 1 Regulaminu posiadacz rachunku powinien posługiwać się hasłami i hasłem dostępu wyłącznie w sposób zapewniający zachowanie ich poufności, w szczególności zobowiązany jest do nieudostępniania haseł i hasła dostępu osobom nieupoważnionym.

Dyspozycje i oświadczenia składane przez posiadacza rachunku za pośrednictwem M. uznaje się za spełniające wymogi formy pisemnej i skutkują one zobowiązaniami i uprawnieniami o treści określonej w komunikatach podanych w Kanałach B.. Dyspozycja oraz oświadczenie złożone poprzez Kanały B., potwierdzone co najmniej osobistym hasłem 1 uważa się za autentyczne.

Niesporne, wynika z:

- umowa rachunku oszczędnościowo-rozliczeniowego z 16.09.2008 r. – k. 14-17,
- regulamin – k. 156-158,
- zeznania powoda – k. 150-153.

W dniu 03 maja 2020 r. A. B. (1) powrócił do domu z pracy, do której wyjeżdża za granicę (marynarz). A. B. (1) pracuje jako marynarz w Brazylii. Podczas wyjazdów do pracy nie korzysta on z zainstalowanie w jego telefonie komórkowym aplikacji pozwalającej na dokonywane operacji na rachunku bankowym. W tym czasie bowiem korzysta on z miejscowej karty telefonicznej i w tym celu z telefonu wyjmuje polska kartę sim i instaluje kartę sim miejscowego operatora. Za granicą nie korzysta on z polskiej karty sim. (...) kartę sim podczas pracy za granica przechowuje on w portfelu, a kiedy przebywa na statku portfel przechowuje w swojej kabinie, która jest zamykana na klucz, do którego tylko on ma dostęp. Osoby nieuprawnione nie mają dostępu do jego kabiny. Jedynie dostęp do kabiny ma obsługa sprzątająca.

Następnego dnia, tj. w dniu 04 maja 2020 r. A. B. (1) około godziny 15:30-15:40 spostrzegł, iż jego telefon komórkowy o numerze (...) nie działa w sposób prawidłowy (nie mógł uzyskać połączeń głosowych). Początkowo był przekonany, iż wynika to z mechanicznego uszkodzenia karty sim powstałego na skutek przekładania karty polskiej i brazylijskiej. Z tego powodu udał się do najbliższego oddziału T-M. w G. mieszczącego się przy ul. (...) M. 31. Tam sprawdzono, ze karta rzeczywiście nie działa i początkowo sprzedawca nie widział jaki jest tego powód. A. B. (1) uzyskał informację, iż karta SIM o numerze (...) okazała się niesprawna, w związku z czym złożył wniosek o wydanie nowej kart sim. O godzinie 17:03 A. B. (2) wydana została nowa karta SIM o numerze (...), która została od razu aktywowana

A. B. (1) dokonał ponownej instalacji aplikacji bankowej na swoim telefonie z nową kartą SIM. Wówczas – po zalogowaniu – zauważył, że z jego rachunków bakowych zaczęły w sposób niekontrowany i nieautoryzowany wypływać środki pieniężne. Skontaktował się z Telefonicznym Biurem (...). Otrzymał informację, że w dniu 04 maja 2020 r., o godzinie 15:41 w salonie (...) w Centrum Handlowym (...), znajdującym się przy ul. (...) 41 w W., został wystawiony duplikat karty SIM o numerze (...) odpowiadający numerowi telefonu powoda. A. B. (1) nie wnosił o wydanie duplikatu karty SIM w salonie w W., w związku z czym powiadomił o zdarzeniu jednostkę policji w G.. W. również o wydanie nowego millekodu oraz ustalił nowe hasło do bankowości elektronicznej.

A. B. (1) niezwłocznie skontaktował się z Bankiem., Poinformował o sytuacji pracownika Banku i zażądał blokady wszelkich operacji wychodzących z należących do niego rachunków bankowych. Całość transakcji nieautoryzowanych opiewała na kwotę 89.000 zł. Znaczną część tych transakcji Bank zdążył zablokować. Ostatecznie A. B. (1) w wyniku transakcji wykonanych w okresie, kiedy nie miał dostępu do swojego numeru telefonu, tj. w okresie od aktywowania

nowej kart sim przez nieznane osoby do jej dezaktywacji utracił z rachunku kwotę 25.000 złotych. W tym kwotę 6.000 złotych wypłaconą za pośrednictwem Blik (wszystkie transakcje wykonane w bankomatach znajdujących się w W. przy ul. (...)), kwotę 12.000 złotych z tytułu wykonanych przelewów na rzecz nieznanych mu osób oraz kwotę 7.000 złotych tytułem transakcji na rzecz D. P.

O godzinie 15:41 wyłączona została karta SIM o numerze (...). Aktywowana została nowa karta SIM o numerze (...), którą powód się nie posługiwał. Następnie, o godzinie 17:03, A. B. (1) deaktywował kartę SIM o numerze (...) i aktywował właściwą dla niego, nową kartę SIM o numerze (...). Nowa karta sim w salonie operatora telefonicznego w W. została wydana na nazwisko A. B. (1) po okazaniu dowodu osobistego na jego nazwisko. W tym czasie A. B. (1) nadal posiadał, w swoim portfelu dowód osobisty. A. B. (1) nigdy nie utracił swojego dowodu osobistego.

W przedziale czasowym od godziny 15:41 do godziny 17:03 A. B. (1) nie miał możliwości korzystania ze swojego telefonu komórkowego, utracił możliwość połączenia się z siecią oraz dokonania autoryzowania jakichkolwiek transakcji płatniczych. Karta SIM należąca do A. B. (1) o numerze (...) była wyłączona w chwili wykonywania nieautoryzowanych transakcji płatniczych przez osoby trzecie.

A. B. (1) w dniu 04 maja 2020r. nie przebywał w W..

Aplikacja służąca do obsługuj bankowości elektronicznej przez nieustalone osoby po zgłoszeniu zaginięcia karty sim została zainstalowana na telefonie marki S.. W tym czasie A. B. (1) używał telefonu marki S.. Zainstalowanie aplikacji na nowym modelu telefonu wymagało podania millekodu oraz hasła.

Dowody:

- wiadomość mail z 05.05.2020 r. – k. 18,
- postanowienie - k. 55-56,
- dane kart SIM wraz z wykazem SMS – k. 143-144,
- zeznania powoda – k. 150-153.

Osoby trzecie, które dysponowały kartą SIM o numerze (...), wydaną dla numeru telefonu powoda (...), dokonały potwierdzenia transakcji sms kodem każdorazowo wysłanym na numer telefonu komórkowego (...) Osoby te usunęły limity transakcji, które ustawia A. B. (1) na swoich rachunkach bankowych.

W dniu 4 maja 2020 r. doszło do formalnie poprawnego logowania w M. na profilu należącym do A. B. (1). Dane identyfikujące wymagane do logowania to ośmiocyfrowy login, indywidualne hasło i dwa losowo wybrane znaki dodatkowego identyfikatora: numeru PESEL, numeru dowodu osobistego lub paszportu. Po zalogowaniu do bankowości elektronicznej dodani zostali odbiorcy zaufani pod nazwami: (...), (...), „B. (...).”, (...). Przelewy do odbiorców zaufanych nie wymagają późniejszego potwierdzenia dodatkowym hasłem.

Dyspozycje dodania odbiorców zaufanych zostały zatwierdzone za pomocą haseł sms wysłanych na numer (...)

Za pośrednictwem aplikacji zainstalowanej na urządzeniu S. (...) zostały zrealizowane wypłaty BLIK z Konta Osobistego P. Klienta na kwoty 4.000 zł oraz 2 x 1.000 zł.

W dniu 04 maja 2020 r. zostały także zrealizowane przelewy z rachunków Klienta:

- z Konta Osobistego P. na rachunek (...), Alias i nazwa odbiorcy: S. T. na kwoty 3 x 3.000 zł, 2.000 zł, 1.000 zł,
- z Konta 360° na rachunek (...), Alias i Nazwa odbiorcy: D. P. na kwotę 7.000 zł.

Przelewy zrealizowane M., zanim zostali dodani odbiorcy zaufani, zostały potwierdzone hasłami sms wysyłanymi na numer telefonu A. B. (1), tj. (...)

A. B. (1) korzysta z telefonu komórkowego marki S..

A. B. (1) nie dokonał osobistej autoryzacji żadnej z ww. transakcji płatniczych.

Dowody:

- potwierdzenia wykonania transakcji – k. 21-49,
- dane kart SIM wraz z wykazem SMS – k. 143-144,
- zeznania powoda – k. 150-153.

Postanowieniem z 31 sierpnia 2020 r.(...) (...) w W. umorzył dochodzenie w sprawie umyślnego przyjęcia4 maja 2020 r. w W. środków pieniężnych w łącznej kwocie 19.000 zł, pochodzących z czynów zabronionych popełnionych na szkodę A. B. (1), które wpłynęły na rachunek bankowy nr (...) prowadzony na rzecz D. P. oraz rachunek nr (...), prowadzony na rzecz S. T.. Nie wykryto sprawcy przestępstwa.

Dowód: postanowienie - k. 55-56.

A. B. (1) wezwał pozwany Bank do zapłaty na jego rzecz kwoty w wysokości 25.000 zł (data doręczenia wezwania 8 czerwca 2020 r.). Następnie pełnomocnik powoda, pismem z 30 września 2020 r., ponownie zawnioskował do Banku o natychmiastowy zwrot środków pieniężnych w wysokości 25.000 zł.

Bank odmówił zwrotu środków, wskazując, iż był zobowiązany wykonać prawidłowo zlecone dyspozycje aktywacji aplikacji oraz realizacji transakcji.

Dowody:

- pismo z 29.06.2020 r. – k. 19-20,
- wniosek o zwrot środków pieniężnych wraz z potwierdzeniem nadania – k. 50-53,
- wezwanie do zapłaty – k. 54.

A. B. (1) nigdy nie udostępniał swojego M. oraz hasła. Nigdy ich nie zapisywał. Znał te numery na pamięć, sam ustalił hasło, które było unikatowe. Przed zdarzeniem z 4 maja 2020 r. A. B. (1) nie otrzymał żadnej wiadomości mailowej z żądaniem logowania do Banku, czy też wiadomości sms z żądaniem podania danych niezbędnych do logowania do Banku. Osobą, która posiada upoważniony dostęp do rachunków bankowych powoda jest jego żona. Nie zna ona jednak loginu i hasła do bakowości elektronicznej, nie ma zainstalowanej aplikacji bankowej na swoim urządzeniu telefonicznym. A. B. (1) nie wchodzi ze swojego komputera na strony internetowe o zwiększonym ryzyku zainfekowania wirusami. Zapoznawał się ze wszystkimi informacjami dotyczącymi bezpieczeństwa logowania się do bankowości internetowej.

W przeciągu około pół roku przed zdarzeniem z 4 maja 2020 r. A. B. (1) nikomu nie udostępniał swojego dowodu osobistego, nie zgubił go. Nigdy wcześniej nie zgubił dowodu osobistego. Dowód osobisty posiadał od 2011 r. Nie skanował, ani nie kserował swojego dowodu osobistego. Nie fotografował dokumentu. Jedynie w 2011 roku Policja skopiował jego dowód osobisty, kiedy ubiegał się o pozwolenie na broń.

A. B. (1) zapoznał się z zasadami dotyczącymi bezpieczeństwa logowania do bankowości elektronicznej. Zawsze wyługowuje się z aplikacji bankowej. Stara się unikać płatności blikiem. Nikomu nie udostępniał hasła i millekodu, nigdzie ich nie zapisywał, albowiem je pamiętał. Jest on wyczulony na kwestię bezpieczeństwa i rachunek ma

zabezpieczony programami antywirusowymi. Przed tym zdarzeniem nie otrzymał żadnego maila z żądaniem logowania do banku czy też wiadomości SMS żądaniem podania danych do logowania do banku. Nie udostępnił również danych do logowania do bankowości internetowej swojej żonie. Ona ma upoważnienie do jego rachunku bankowego, ale nie ma dostępu do bankowości internetowej, w tym nie ma zainstalowanej aplikacji służącej do korzystania z bankowości internetowej.

A. B. (1) jest marynarzem, wyjeżdża do pracy za granicę. Gdy przebywa w Brazylii, to korzysta z lokalnej karty SIM, zaś polską kartę SIM przechowuje w portfelu. Portfel pozostawia w kabinie, która zamykana jest kluczem kodowym. Do kabiny dostęp ma jedynie obsługa sprzątająca.

Dowód: zeznania powoda – k. 150-153.

Sąd zważył co następuje.

Powództwo zasługiwało na uwzględnienie w całości.

Opisany wyżej stan faktyczny Sąd ustalił w oparciu o przedstawione przez strony niniejszego postępowania dowody z dokumentów, udostępniony przez (...) S.A. dane kart SIM oraz wykaz sms przychodzących na numer (...)Do rekonstrukcji stanu faktycznego sprawy posłużył nadto Sądowi dowód z przesłuchania powoda A. B. (1). Podkreślić należy, iż Sąd nie miał podstaw do kwestionowania złożonych w niniejszej sprawie zeznań przez powoda A. B. (1). Jego zeznania są spójnie i nie zawierają żadnych sprzeczności. Poza tym znajdują one potwierdzenie w innym zgromadzonym w sprawie materiale dowodowym w postaci dokumentów. Również pozwany, mimo ogólne kwestionowania podawanych przez powoda okoliczności faktycznych nie zaprezentował żadnych dowodów, które podważyłby w jakikolwiek sposób podane przez powoda okoliczności, zwłaszcza w zakresie zachowania przez powoda w ramach korzystania z bankowości elektronicznej należytej staranności w zakresie bezpieczeństwa logowania do jego rachunku bankowego. Zwłaszcza że pozwany w skierowanym do powoda przed wszczęciem postępowania piśmie w zasadzie potwierdza, iż doszło do zainstalowania na nowym telefonie aplikacji do obsługi bankowości elektronicznej dotyczącej rachunku bankowego powoda, jak również potwierdził, iż doszło do niekontrolowanego wypływu środków z rachunku powoda, a jedynie nie znalazł podstaw do przyjęcia odpowiedzialności za zaistniała sytuację. Z tych też względów brak jest podstaw do kwestionowania zeznań powoda, zwłaszcza że wraz z dowodami z dokumentów tworzą logiczny obraz zaistniałego stanu faktycznego w sprawie. Dokumenty, które legły u podstaw ustaleń, Sąd uznał w całości za autentyczne i wiarygodne. Żadna ze stron nie kwestionowała przedmiotowych dowodów od strony ich formy czy treści, a nie ujawniły się też jakiekolwiek okoliczności, które dawałyby podstawę do dokonania z urzędu negatywnej oceny tych dokumentów. Stąd też omawiane dowody zachowują w pełni właściwą dla siebie moc dowodową nadaną przepisami art. 244 i 245 k.p.c. Sąd nadto przyznał walor wiarygodności zeznaniom powoda, które korespondują ze zgromadzonymi w toku postępowania pozostałym materiałem dowodowym i tworzą spójny obraz zdarzeń, do których doszło w dniu 04 maja 2020 r..

Żądanie pozwu obejmuje zwrot kwoty nieautoryzowanych transakcji płatniczych dokonanych w dniu 04 maja 2020 r. z rachunków bankowych należących do powoda, prowadzonych w Banku (...) Spółce Akcyjnej z siedzibą w W..

W pierwszej kolejności odnieś należy się do zgłoszonego przez stronę pozwaną zarzutu w przedmiocie braku po jej stronie legitymacji biernej, albowiem posiadanie przez strony legitymacji czynnej i biernej w procesie jest przesłanką zasadniczą, od której istnienia uzależniona jest możliwość uwzględnienia powództwa, a jej brak, zarówno w postaci czynnej jak i biernej, prowadzi do wydania wyroku oddalającego powództwo.

Wskazać należy, że legitymacja procesowa to uprawnienie do poszukiwania ochrony prawnej w konkretnej sprawie. Legitymacja czynna zawsze ściśle jest związana ze strona powodową i oznacza jej uprawnienie do wszczęcia i prowadzenia procesu. Legitymacja bierna uzasadnia występowanie w procesie w charakterze pozwanego. Legitymacja procesowa to zatem uprawnienie konkretnego podmiotu (legitymacja czynna) do występowania z konkretnym roszczeniem przeciwko innemu oznaczonemu podmiotowi (legitymacja bierna) wypływająca z prawa materialnego.

Strona pozwana swój zarzut uzasadniała w ten sposób, iż podstawa żądania powoda powinna mieć swoje źródło w działaniu operatora telekomunikacyjnego, Bank nie może ponosić odpowiedzialności za to, że operator telekomunikacyjny może wydać duplikat karty SIM innej osobie. Tak też brak winy w wykonaniu nieautoryzowanych transakcji ma zdaniem pozwanej uzasadniać brak legitymacji biernej po jej stronie.

W ocenie Sądu argumentacja pozwanej jest nietrafiona, a podniesiony zarzut braku legitymacji biernej ocenić należało jako bezzasadny i podzielić w całości w tymże zakresie stanowisko strony powodowej. P. bowiem należy, iż powód w niniejszej sprawie nie domaga się odszkodowania za szkody powstałe na skutek wydania nieupoważnionej osobie nowej karty sim, lecz domaga się zwrotu kwot nieautoryzowanych transakcji dokonanych z rachunku powoda, który prowadzony był w pozwanym Banku. Tym samym do dokonania zapłaty tych kwota na takiej podstawie może być jedynie Bank, a nie inny podmiot. Tym samym w niniejszej sprawie można jedynie rozważać brak odpowiedzialności Banku za dokonanie nieautoryzowanych transakcji, a nie brak legitymacji biernej.

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. W myśl zaś art. 726 k.c. na banku spoczywa obowiązek zwrotu wolnych środków pieniężnych na każde żądanie, chyba że umowa uzależnia obowiązek zwrotu od wypowiedzenia.

Mając na względzie powyższe nieodzownym pozostaje odniesienie się również do przepisów ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (Dz.U.2011, Nr 199, poz. 1175 z późń. zm., w dalszej części u.u.p.), która określa prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych oraz zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych.

Ustawa z dnia 19 sierpnia 2011 roku o usługach płatniczych statuuje podstawową zasadę, że dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika. Ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową.

Powołane powyżej przepisy ustawy o usługach płatniczych bezpośrednio przesądzając kwestię występowania legitymacji biernej po stronie pozwanego Banku.

Stan faktyczny w niniejszej sprawie był w gruncie rzeczy w dużej mierze niesporny. Najistotniejszą sporną okolicznością było to, czy powód wykazał się rażącym niedbalstwem w korzystaniu z bankowości elektronicznej, przechowywaniu loginu , hasła, pinkodu, karty SIM do telefonu komórkowego podczas wyjazdów do pracy za granicę.

Rozstrzygając przedmiotową kwestię sąd zobowiązany był wziąć pod uwagę przepisy zawarte w ww. ustawie z 19 sierpnia 2011 r. o usługach płatniczych.

Na pozwanym Banku, jako dostawcy wydającemu instrument płatniczy, ciążył z mocy art. 43 pkt 1 ustawy obowiązek zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, na powodzie zaś - jako użytkowniku instrumentu płatniczego - spoczywał obowiązek korzystania z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu (art. 42 ust. 1 pkt 1 i 2). W celu spełnienia powyższego obowiązku użytkownik, z chwilą otrzymania instrumentu płatniczego, winien podejmować niezbędne środki zapobiegające naruszeniu indywidualnych zabezpieczeń instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (art. 42 ust. 2).

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 (por. wyrok SN z dnia 14 kwietnia 2003 roku, I CKN 308/01, Legalis nr 61218).

W rozumieniu wskazanego aktu (art. 4 ust. 1 ust. 2 pkt 1 u.u.p.) bank krajowy jest dostawcą usług płatniczych rozumianych jako działalność polegająca w szczególności na wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy przez wykonywanie usług polecenia przelewu, w tym stałych zleceń (art. 3 pkt 2 lit. c u.u.p.). Płatnikiem w rozumieniu ustawy jest m.in. osoba fizyczna, składająca zlecenie płatnicze, czyli oświadczenie skierowane do dostawcy zawierające polecenie wykonania transakcji płatniczej (art. 2 pkt 22 i pkt 36 u.u.p.). Zlecenie płatnicze składane jest zaś przez płatnika przy użyciu instrumentu płatniczego, którym jest zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego (art. 2 pkt 10 u.u.p.).

Stosownie do treści art. 46 ust. 1 u.u.p. w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku, gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

W myśl zaś art. 45 ust. 1 u.u.p. ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Należy mieć jednak na uwadze, że wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 (art. 45 ust. 2 u.u.p.).

Transakcja płatnicza nosi przymiot autoryzowanej wówczas, gdy płatnik wyrazi zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie pomiędzy płatnikiem a jego dostawcą (art. 40 ustęp 1 u.u.p.). Jednocześnie zgodnie z treścią art. 43 pkt 1 u.u.p. dostawca wydający instrument płatniczy jest obowiązany do zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Z obowiązkiem tym skorelowana jest powinność użytkownika instrumentu płatniczego do korzystania z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. W tym celu użytkownik, z chwilą otrzymania instrumentu płatniczego, winien podejmować niezbędne środki zapobiegające naruszeniu indywidualnych zabezpieczeń instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (art. 42 ust. 1 punkt 1 i 2 u.u.p.).

W tym miejscu należy wskazać, że implementowana do porządku krajowego dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 roku w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, (...), (...) i (...) i uchylająca dyrektywę 97/5/WE (Dz.U.UE. L 319/1) zawiera sformułowanie transakcja „autentykowana", podczas gdy polski ustawodawca posługuje się zwrotem transakcja „autoryzowana". Warto jednak podkreślić, że zgodnie z art. 288 ust. 3 Traktatu o Funkcjonowaniu Unii Europejskiej (w dalszej części (...)) dyrektywa wiąże każde Państwo Członkowskie, do którego jest kierowana, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawia jednak organom krajowym swobodę wyboru formy i środków. Jednym z celów Dyrektywy 2007/64/WE z dnia 13 listopada 2007 roku było zmniejszenie ryzyka i konsekwencji nieautoryzowanych lub nieprawidłowo wykonanych usług płatniczych z punktu widzenia użytkownika usług płatniczych, którym w przeważającej części przypadków pozostaje konsument. I tak w treści preambuły do

przedmiotowej Dyrektywy ustawodawca europejski zaznaczył m.in., że ocena ewentualnego zaniedbania ze strony użytkownika usług płatniczych winna uwzględnić wszystkie okoliczności. Oczywistość i stopień domniemanego zaniedbania powinien ocenić sąd zgodnie z prawem krajowym. Warunki umowne dotyczące wydania i korzystania z instrumentu płatniczego, których skutkiem byłoby zwiększenia ciężaru dowodu spoczywającego na konsumencie lub zmniejszenie ciężaru dowodu spoczywającego na wydawcy, powinny być uznane za nieważne (pkt 33 preambuły). Nadto Państwa członkowskie powinny mieć możliwość ustalenia zasad mniej rygorystycznych niż zasady określone powyżej w celu utrzymania istniejącego poziomu ochrony konsumentów i propagowania zaufania do bezpiecznego korzystania z elektronicznych instrumentów płatniczych. Fakt, że różne instrumenty płatnicze wiążą się z różnymi rodzajami ryzyka, powinien być odpowiednio uwzględniany, co powinno pomóc w propagowaniu wydawania bezpieczniejszych instrumentów. Powinno zezwolić się państwom członkowskim na ograniczenie lub zupełne wyłączenie odpowiedzialności płatnika, z wyjątkiem sytuacji, w których płatnik działał w nieuczciwych zamiarach (pkt 34 preambuły). Istotnie w angielskojęzycznej wersji przedmiotowej Dyrektywy, a mianowicie art. 59 ust. 1 użyto sformułowań „authorised" oraz „authenticated", przy czym w ust. 2 tego przepisu użyto wyłącznie zwrotu „authorised". Zarówno w polskojęzycznej, jak i angielskojęzycznej wersji dokumentu bezspornie jednak przyjęto, że samo użycie instrumentu płatniczego niekoniecznie jest wystarczające do udowodnienia, że transakcja płatnicza została przez płatnika usług płatniczych autoryzowana (ust.2). Co więcej, gdyby nawet próbować forsować tezę o niewłaściwym tłumaczeniu zwrotu „authenticated" na gruncie art. 59 ust. 1, nie można stracić z pola widzenia, że implementacja Dyrektywy została dokonana w ramach ustawy o usługach płatniczych, na gruncie której ustawodawca polski był w pełni uprawniony do zastosowania bardziej rygorystycznych zapisów mających realizować cel aktu prawnego Unii Europejskiej. Innym słowy harmonizacja przepisów na poziomie Państw Członkowskich jest instrumentem realizującym podstawowy cel Dyrektywy, przy czym każde z Państw Członkowskich dysponuje swobodą formy i środków, które mają ten rezultat uzyskać. O ile uzasadnionym pozostawałoby powoływanie się na brak realizacji tego celu w ramach implementacji lub osiągnięcia rezultatu nieodpowiadającego wyznaczonym standardom, o tyle chybioną pozostaje argumentacja o zastosowaniu środków bardziej restrykcyjnych niż przewidziane, w szczególności w kontekście treści preambuły oraz prokonsumenckiej wykładni przepisów w relacjach konsumenta z profesjonalistą.

Przenosząc treść powyższych regulacji na płaszczyznę przedmiotowej sprawy rozstrzygnięciu podlega kwestia, czy sporne transakcje płatnicze były autoryzowane przez A. B. (1) w dniu 4 maja 2020 r.

Zgromadzony materiał dowodowy bezsprzecznie prowadzi do wniosku, że 4 maja 2020 r. nieustalona osoba/ nieustalone osoby trzecie, które dysponowały kartą SIM o numerze (...), wydaną dla numeru telefonu powoda (...) w salonie (...) w W., dokonały potwierdzenia transakcji sms kodem każdorazowo wysłanym na numer telefonu komórkowego (...) Osoby te usunęły limity transakcji, które ustawia A. B. (1) na swoich rachunkach bankowych. Ponadto doprowadziły do poprawnego logowania w M. na profilu należącym do A. B. (1). Po zalogowaniu do bankowości elektronicznej dodani zostali odbiorcy zaufani pod nazwami: (...), (...), „B. (...).", (...). Dyspozycje dodania odbiorców zaufanych zostały zatwierdzone za pomocą haseł sms wysłanych na numer (...) Za pośrednictwem aplikacji zainstalowanej na urządzeniu S. (...) zostały zrealizowane wypłaty BLIK z Konta Osobistego P. Klienta na kwoty 4.000 zł oraz 2 x 1.000 zł.

W dniu 04 maja 2020 r. zostały także zrealizowane przelewy z rachunków powoda: z Konta Osobistego P. na rachunek (...), Alias i nazwa odbiorcy: S. T. na kwoty 3 x 3.000 zł, 2.000 zł, 1.000 zł; z Konta 360° na rachunek (...), Alias i Nazwa odbiorcy: D. P. na kwotę 7.000 zł

Na podstawie zgormadzonego w sprawie materiału dowodowego Sąd ustalił, iż A. B. (1) nie dokonał osobistej autoryzacji żadnej z ww. transakcji płatniczych. W przedziale czasowym od godziny 15:41 do godziny 17:03 powód bowiem nie mógł korzystać ze swojego telefonu komórkowego, utracił możliwość połączenia się z siecią oraz dokonania autoryzowania jakichkolwiek transakcji płatniczych. Karta SIM należąca do A. B. (1) o numerze (...) była wyłączona w chwili wykonywania nieautoryzowanych transakcji płatniczych przez osoby trzecie. Ponadto 4 maja 2020 r. A. B. (1) nie przebywał w W.. A. B. (1) nie doprowadził w jakikolwiek sposób do udostępnienia swoich danych dotyczących logowania do rachunku bankowego innym osobom i w żaden sposób nie uczestniczył w wykonaniu transakcji kwestionowanych w niniejszym postępowaniu. Jak już bowiem wskazano wyżej przepis art. 45 ust. 1 w/

w ustawy o usługach płatniczych stanowi, że ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika spoczywa na dostawcy tego użytkownika, przy czym do zrealizowania tego obowiązku dowodowego nie jest wystarczające wykazanie samego zarejestrowanego użycia instrumentu płatniczego, tj. jak niniejszej sprawie wykazania, że doszło do autoryzowania transakcji poprzez zastosowanie procedury jej autoryzacji określonej w umowie czy też poprzez dokonanie autoryzacji czynności przesłanymi na numer telefonu powoda kodem SMS. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie i wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych. W niniejszej zaś sprawie niewątpliwie w okresie dokonywania kwestionowanych czynności powód w sposób obiektywny nie mógł dokonać potwierdzenia żadnych czynności, albowiem dokonano w sposób nieuprawniony dezaktywowania karty sim w jego telefonie i zainstalowania na nową (wydana innym osobom) kartę sim aplikacji do bankowości internetowej. Przypomnieć przy tym należy, że transakcję płatniczą uważa się za autoryzowaną tylko wówczas, jeżeli płatnik wyraził zgodę na jej wykonanie, a zatem samo formalne zastosowanie procedury autoryzacji nie jest wystarczające od uznania, że transakcja została przez powoda autoryzowana. Ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża więc bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową.

Uwzględniając powyższe Sąd stwierdził brak podstaw do uznania, że transakcje płatnicze z dnia 04 maja 2020 roku były autoryzowane przez A. B. (1). Czynności te z punktu widzenia systemu informatycznego Banku były przeprowadzone poprawnie, przy wykorzystaniu właściwych narzędzi autoryzacyjnych., mimo tego transakcji płatniczych wykonanych z konta powoda w dniu 04 maja 2020 r. nie można uznać za transakcje autoryzowane.

Uwzględniając powyższe argumenty należy ponownie odnieść się do treści art. 45 ust. 2 u.u.p. należy podkreślić, że ryzyko zarejestrowanego użycia instrumentu płatniczego nieautoryzowanego przez klienta obciąża bank, o ile tylko klient nie doprowadził do nieautoryzowanej transakcji umyślnie albo na skutek rażącego niedbalstwa wiążącego się z naruszeniem obowiązków określonych w art. 42 ustawy. Innymi słowy, jeżeli do nieautoryzowanej transakcji doszło na skutek ingerencji przestępców w sprzęt lub oprogramowanie klienta, z woli ustawodawcy ryzyko takiego stanu rzeczy ponosi bank, o ile tylko klientowi nie można przypisać umyślności lub rażącego niedbalstwa. Regulacja ta musi być na gruncie postępowania cywilnego oceniona w kontekście art. 6 k.c. Zgodnie bowiem z obowiązującą zasadą ciężaru dowodu (onus probandi) strona winna udowodnić fakty, z których wywodzi korzystne dla siebie skutki prawne. W niniejszej sprawie oznacza to, że pozwany bank zobowiązany był wykazać autoryzowanie transakcji z 4 maja 2020 r. przez A. B. (1), czego ostatecznie nie uczynił.

Rażące niedbalstwo (culpa lata) jest kwalifikowaną postacią winy nieumyślnej Oznacza zatem wyższy jej stopień niż w przypadku zwykłego niedbalstwa, leżący już bardzo blisko winy umyślnej (culpa lata dolo aequiparatur). Wykładnia pojęcia rażącego niedbalstwa powinna uwzględniać kwalifikowaną postać braku zwykłej staranności w przewidywaniu skutków. Konieczne jest zatem stwierdzenie, że podmiot, któremu taką postać winy chce się przypisać, zaniedbał takiej czynności zachowującej chronione dobro przed zajściem zdarzenia powodującego szkodę, której niedopełnienie byłoby czymś absolutnie oczywistym w świetle doświadczenia życiowego dostępnego każdemu przeciętnemu uczestnikowi obrotu prawnego i w sposób wprost dla każdego przewidywalny mogło doprowadzić do powstania szkody. Rażące niedbalstwo zachodzi bowiem tylko wtedy, gdy stopień naganności postępowania drastycznie odbiega od modelu właściwego w danych warunkach zachowania się dłużnika (por. wyrok Sądu Najwyższego z dnia 22 kwietnia 2004 roku, II CK 142/03, Lex nr 484721, wyrok Sądu Najwyższego z dnia 25 września 2002 roku, I CKN 969/00, LEX nr 55508, wyrok (...)z dnia 20 marca 2017 roku, (...), orzeczenia.lodz.so.gov.pl, wyrok (...) z dnia 2 maja 2017 roku, (...), orzeczenia.lodz.so.gov.pl, wyrok Sądu Okręgowego w Łodzi z dnia 22 marca 2016 roku,(...), Lex nr 2130586).

Podzielając w pełni powyżej zaprezentowane poglądy judykatury nie sposób mówić o niedbałym zachowaniu powoda, a do tego w stopniu rażącym. Podkreślić należy w pierwszej kolejności, iż pozwany mimo ogólnego kwestionowania swojej odpowiedzialności , którą wywodził z faktu autoryzowania dokonanych transakcji, w żadne sposób nie

wykazał, aby zaistniała sytuacja była skutkiem zawinione działania powoda, w tym jego rażącego niedbalstwa. Zresztą przeprowadzone w sprawie postępowanie dowodowe nie pozwala na przypisanie powodowi takiego właśnie zachowania. Powód bowiem jak wynika z jego zeznań, które nie zostały w żadne sposób podważone żadnym dowodem ze strony pozwanego, w sposób bezpieczny i rozsądny korzystał w bankowości internetowej. Korzystał jedynie aplikacji na telefonie bądź z własne komputera, jak również zabezpieczał się programami antywirusowymi. Nikomu nie udostępniał żadnych danych niezbędnych do logowania do bankowości internetowej, w tym nawet swojej żonie, która miała upoważnienie do jego rachunku bankowego. Nie korzystał również z bankowości internetowej „ polskiej" kart SIM podczas pobyty w pracy za granicą. Nie zapisywał również danych dostępu do logowania do konta, co mogłoby narazić na utratę tych danych. Nie udostępniał również nikomu nieuprawnionemu swojego dowodu osobistego w celu dokonania jego kopii czy też zeskanowania. W tej też sytuacji nie sposób uznać, aby można było przypisać powodowi jakiekolwiek rażące niedbalstwo w zakresie wykonywania nałożonych na niego obowiązków z umowy rachunku bankowego, w szczególności w zakresie korzystania z bankowości elektronicznej. Jak również nie sposób w realiach niniejszej sprawy uznać aby naruszył on jakiekolwiek obowiązki wynikające z tej umowy. Podkreślić przy tym należało, iż to na pozwanym w tym zakresie spoczywał obowiązek dowody, zaś pozwany nie tylko nie wskazał na czym miałoby podlegać rażące niedbalstwo w działaniu powoda, lecz również w tym zakresie nie wykazał żadnej inicjatywy dowodowej.

Nie bez znaczenia tutaj pozostaje postawa samego pozwanego Banku w zakresie wykonania z rachunku bankowego powoda nieautoryzowanych transakcji płatniczych. Wskazać bowiem należy, iż Bank nie zareagował w zasadzie w żaden sposób na nagły wzrost transakcji na rachunku bankowym powoda polegających na dokonywaniu licznych i w bardzo krótkim czasie wypłat na łączną bardzo wysoką kwotę, która wynosił około 89.000 złotych. Zwłaszcza że bezpośrednio przed ich dokonaniem nastąpiła zmiana modelu telefonu komórkowego i ponowne zainstalowanie aplikacji do obsługi bankowości elektronicznej, a nadto przelewy były wykonywane „seriami" na rzecz tych samych osób. To zaś zdaniem Sądu w dostateczny sposób uzasadniało podejrzenie nieuprawnionej ingerencji w rachunek bankowy powoda. Dopiero interwencja powoda polegająca na zgłoszeniu dokonywania z jego rachunku nieautoryzowanych transakcji spowodowała, iż część z ich została wstrzymana.

Zważyć również należy, iż w niniejszej sprawie nie sposób również zarzucić powodowi jakichkolwiek zaniedbań po uzyskaniu informacji o niekontrolowanym wypływie środków z jego rachunku bankowego w okresie, kiedy nie mógł korzystać z telefonu. Powód bowiem od razu po powzięciu tej wiadomości zgłosił ten fakt Bankowi co umożliwiło zablokowanie niewykonanych dotychczas transakcji na znaczną kwotę. Od razu również po stwierdzeniu niedziałania telefonu poszedł wyjaśnić sytuację u operatora telefonii komórkowej. Dokonał również zgłoszenia odpowiednim służbom, w tym dokonał zgłoszenia na Policji.

W tak ukształtowanym stanie faktycznym Sąd stwierdził brak podstaw do uznania spornych transakcji za autoryzowane przez powoda, oceny zachowania A. B. (1) jako umyślnego lub cechującego się rażącym niedbalstwem, a także jego przyczynienia się do powstałej szkody w rozumieniu art. 362 k.c.

W świetle poczynionych rozważań uzasadnionym pozostawało żądanie zwrotu środków pieniężnych z transakcji, które nie były autoryzowane przez powoda. Tym samym na rzecz powoda przyznano kwotę 25.000 zł. Umowa rachunku bankowego sformułowana została przez bank i skoro zapewnił on posiadacza rachunku, że na każde wezwanie wypłaci zgromadzone na rachunku środki musi obecnie tak uczynić, bowiem dokonanie wypłaty na rzecz innych osób, stanowiło nienależytą realizację umowy.

O odsetkach sąd orzekł na podstawie art. 481 k.c. w zw. z art. 46 ust. 1 u.u.p. zgodnie z żądaniem powoda tj. od 01 lipca 2020 roku.

Orzeczenie o kosztach procesu Sąd oparł na treści art. 98 § 1 k.p.c., który ustanawia ogólną zasadę, iż strona przegrywająca sprawę obowiązana jest zwrócić przeciwnikowi na jego żądanie koszty niezbędne do celowego dochodzenia praw i celowej obrony – koszty procesu. W niniejszej sprawie Sąd w całości uwzględnił powództwo, dlatego też to strona pozwana jest tą stroną procesu, która przegrała przedmiotową sprawę, w związku z tym

obowiązana jest zwrócić powodowi poniesione przez niego koszty procesu. Warunkiem zasądzenia od strony przegrywającej na rzecz przeciwnika kosztów procesu jest zgłoszenie żądania, który w niniejszej sprawie został spełniony, albowiem wniosek taki zgłoszony został już w pozwie. W skład kosztów należnych stronie powodowej wchodzą: opłata sądowa od pozwu w wysokości 1.000 zł, wynagrodzenie adwokata w kwocie 3.600 złotych oraz opłata od pełnomocnictwa procesowego w kwocie 17 zł.

Mając na uwadze powyższe, na podstawie art. 98 § 1 k.p.c. orzeczono jak w punkcie II. wyroku.

(...)(...)

Sygn. akt(...)

(...)

1. (...) (...)
2. (...)(...)
   - (...)
3. (...) (...)

G.,(...)

(...) (...)