Sygnatura akt I C 477/21

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Pleszew, dnia 16 listopada 2022 r.

Sąd Rejonowy w Pleszewie I Wydział Cywilny w następującym składzie:

Przewodniczący: sędzia Izabela Ozdowska-Chojnacka

Protokolant: Ewelina Mielcarek

po rozpoznaniu na rozprawie w dniu 17 października 2022 r. w Pleszewie

sprawy z powództwa A. B.

przeciwko (...) BANK (...) Spółka Akcyjna w K.

o zapłatę

1. zasądza od pozwanego (...) BANK (...) Spółka Akcyjna w K. na rzecz powódki A. B. kwotę 33.691,00 zł (trzydzieści trzy tysiące sześćset dziewięćdziesiąt jeden złotych 00/100) z odsetkami ustawowymi za opóźnienie obliczanymi od dnia 06 maja 2021 r. do dnia zapłaty

2. w pozostałym zakresie powództwo oddala

3. kosztami postępowania obciąża w całości pozwanego i z tego tytułu zasądza od niego na rzecz powódki kwotę 5.302,00 zł (pięć tysięcy trzysta dwa złote 00/100), w tym kwotę 3.600,00 zł (trzy tysiące sześćset złotych 00/100) tytułem zwrotu kosztów zastępstwa procesowego

Izabela Ozdowska-Chojnacka

Sygn. akt ***I C 477/21***

UZASADNIENIE

Pozwem z dnia 01 lipca 2021 r. powódka A. B. wniosła o zasądzenie od pozwanego (...) Bank (...) Spółka Akcyjna z siedzibą w K. kwoty 33.691,00 zł wraz z odsetkami ustawowymi za opóźnienie od dnia 01 kwietnia 2021 r. do dnia zapłaty. Nadto wniosła o zasądzenie zwrotu kosztów procesu, w tym zwrotu kosztów zastępstwa procesowego według norm przepisanych.

W uzasadnieniu wskazała, iż dochodzi zapłaty z tytułu zwrotu nieautoryzowanych przez nią transakcji płatniczych z dnia 30 marca 2021 r., dokonanych z jej rachunku przez pozwany bank. Powołała się na umowę rachunku bankowego i przepisu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych.

W odpowiedzi na pozew pozwany (...) Bank (...) Spółka Akcyjna z siedzibą w K. wniósł o oddalenie powództwa w całości oraz o zasądzenie od powódki na jego rzecz zwrotu kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych.

W uzasadnieniu podniósł, iż powódka swoim działaniem umożliwiła osobom trzecim pobranie pieniędzy z jej rachunku bankowego, ponieważ przy dokonywanej transakcji nie zostały przełamane żadne zabezpieczenia banku. Wyjaśnił, iż to powódka samodzielnie i bezpośrednio doprowadziła do autoryzacji przelewów. Zarzucił jej rażące niedbalstwo, gdyż powinna upewnić się czy transakcja, którą autoryzuje jest prawidłowa.

Pełnomocnik powódki cofnął wnioski o przesłuchanie powódki i P. B..

W toku sprawy strony podtrzymały swoje stanowiska.

Sąd ustalił następujący stan faktyczny:

Powódkę M. B. i pozwanego (...) Bank (...) Spółka Akcyjna w K. łączyła umowa rachunku bankowego o numerze (...). W ramach tej umowy powódka korzystała z usług bankowości internetowej. Zgodnie z § 7 ust. 1, 2, 3, 6, Regulaminu świadczenia usług systemu bankowości internetowej, obowiązującym w pozwanym banku od 14 marca 2021 r., użytkownik loguje się do systemu bankowości internetowej osobiście, używając wyłącznie własnych danych, które go uwierzytelniając (np. loginu, który nadał bank). Uwierzytelnienie użytkownika jest wymagane zarówno podczas logowania się do systemu, w tym aplikacji mobilnej jak i podczas inicjowania elektronicznej dyspozycji płatniczej. Z zastrzeżeniem ust. 3 i 4 uwierzytelnianie użytkownika podczas logowania do systemu bankowości internetowej obejmuje czynności: 1) podanie poprawnego loginu, 2) podanie hasła w formie maskowanej, co oznacza podanie przez użytkownika losowo wskazanych przez System znaków składających się na hasło, 3) a w przypadku, gdy jest to wymagane prawem lub wynika ze względów bezpieczeństwa dodatkowo także – podanie odpowiedniego kodu autoryzacyjnego. Jeżeli podczas logowania się użytkownika do Systemu, Bank wymaga podania wszystkich informacji, o których mowa w pkt 1)-3) nazywa się to silnym uwierzytelnianiem. Bank stosuje silne uwierzytelnianie, gdy jest to wymagane przepisami prawa.

Uwierzytelnianie użytkownika podczas logowania do aplikacji mobilnej wymaga wykonania następujących czynności na zaufanym urządzeniu mobilnym: 1) podania poprawnego loginu - przy pierwszym logowaniu, a przy kolejnych logowaniach - Bank może wymagać podania czterech ostatnich znaków loginu, 2) podania hasła w formie maskowanej - przy pierwszym logowaniu, a przy kolejnych logowaniach - podania kodu PIN (..). W celu przeciwdziałania nieuprawionym logowaniom Bank ma prawo wprowadzić dodatkowe środki lub sposoby uwierzytelniania użytkownika podczas logowania do Systemu i aplikacji mobilnej. Bank może wprowadzić dodatkowe środki uwierzytelniania, również gdy będzie to wynikało z przepisów prawa. W przypadku, gdy użytkownik korzysta z zaufanego urządzenia mobilnego Bank przyjmuje, że każda dyspozycja wydana za pomocą tego urządzenia została wydana przez użytkownika, przy wykonaniu czynności uproszczonego uwierzytelnienia. Wobec powyższego z chwilą dodania urządzenia do listy, użytkownik jest zobowiązany do szczególnej, podwyższonej staranności w przechowywaniu takiego urządzenia i nieudostępnianiu go osobom trzecim. Wykaz rodzajów dyspozycji, które są realizowane przez Bank w oparciu o uwierzytelnienie użytkownika dokonywane przez powiązanie jego osoby z urządzeniem mobilnym, które dodał do listy zawiera Komunikat.

W § 11 pkt 1 -2 Regulaminu przewidziano, że Bank wykonuje transakcje płatnicze po ich autoryzacji przez użytkownika. Autoryzacja zlecenia płatniczego przez użytkownika oznacza jego zgodę na wykonanie transakcji płatniczej. Zgody na wykonanie transakcji płatniczej użytkownik może również udzielić za pośrednictwem odbiorcy, dostawcy odbiorcy albo dostawcy świadczącego usługę inicjowania transakcji płatniczej.

Autoryzacja dyspozycji, w tym zleceń płatniczych składanych przez użytkownika za pomocą Systemu bankowości internetowej, w tym aplikacji mobilnej obejmuje: 1) wybranie przycisku akceptacji – gdy Bank uzna, że dana dyspozycja, ze względu na zasady bezpieczeństwa może zostać w ten sposób autoryzowana, albo 2) wybranie przycisku akceptacji w aplikacji mobilnej (autoryzacja mobilna) – gdy Bank uzna, że dana dyspozycja powinna zostać autoryzowana w aplikacji mobilnej. Ten sposób autoryzacji wymaga jednocześnie fizycznego posiadania przez użytkownika zaufanego urządzenia mobilnego, na którym jest zainstalowana i aktywowana aplikacja mobilna, lub 3) podanie poprawnego kodu lub kodów autoryzacyjnych, w tym identyfikatora biometrycznego 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, lub 4) podanie poprawnego kodu lub kodów autoryzacyjnych, w tym identyfikatora biometrycznego oraz zbliżenie urządzenia mobilnego do terminalu.

Bank dostarcza użytkownikowi kody autoryzacyjne, które są kodami SMS, w wiadomości SMS na wskazany wcześniej przez użytkownika telefon do autoryzacji.

W myśl § 32 ust. 3 Regulaminu przewidziano, Bank ponosi odpowiedzialność za ewentualne skutki wykonania transakcji przez osoby trzecie, po dokonaniu zgłoszenia, o jakim mowa w § 35 ust. 6 pkt 1) i złożeniu przez użytkownika dyspozycji blokady dostępu do Systemu, począwszy od: 1) wpłynięcia dyspozycji do Banku - w przypadku, gdy dyspozycję złożono przez System, 2) pisemnego potwierdzenia przez Bank faktu złożenia takiej dyspozycji - w przypadku, gdy dyspozycję złożono w placówce bankowej realizującej tę czynność, 3) uzyskania przez użytkownika ustnego potwierdzenia ze strony infolinii blokady dostępu do Systemu – w przypadku, gdy dyspozycję złożono przez infolinię, - chyba że użytkownik doprowadził umyślnie do nieautoryzowanej transakcji.

Zgodnie z § 34 ust. 3 wymienionego Regulaminu, klienta obciążają w pełnej wysokości nieautoryzowane transakcje płatnicze, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia, co najmniej jednego z obowiązków, o których mowa w § 35 ust. 6-8 oraz § 36 ust. 1-6, § 37 ust. 1.

Z kolei zgodnie z § 36 ust. 1, 2, 5 w/w Regulaminu, użytkownik zobowiązany jest do zapamiętania lub przechowywania hasła oraz innych danych służących do uwierzytelniania i autoryzacji w bezpiecznym miejscu. Użytkownik powinien dokonywać okresowo zmiany hasła.

Użytkownik jest zobowiązany do utrzymania w poufności wszystkich danych służących do jego uwierzytelniania lub autoryzacji przez System oraz nie ujawniania tych danych jakimkolwiek innym osobom, nawet jeśli osoba ta jest inną osobą uprawnioną do rachunku oraz podmiotom nieuprawnionym.

Użytkownik, aby upewnić się, że rzeczywiście nawiązał połączenie z serwerem Banku powinien sprawdzić certyfikat serwera. Bank podaje w Komunikacie nazwę podmiotu, który jest wystawcą serwera bankowego o nazwie (...) lub (...). Sposób weryfikacji wiarygodności certyfikatu Banku oraz inne ważne informacje dotyczące bezpieczeństwa Systemu oraz sposobów zabezpieczania komputera użytkownika podane są na stronie internetowej Banku, w części dotyczącej Systemu bankowości internetowej. Użytkownik zobowiązany jest zabezpieczyć używane urządzenie elektroniczne, w tym mobilne oraz używane oprogramowanie programem antywirusowym.

(Dowód: niesporne, zaświadczenie o posiadaniu konta k. 36-37, regulamin k. 71-101, 124-153)

Powódka jako użytkownik Internetu korzystała z portalu ogłoszeniowego (...) (dostępnego w domenie internetowej (...)). Poprzez ten portal (...) ogłoszenie o sprzedaży bluzy. Wystawiając ogłoszenie podała opis wystawionego przedmiotu oraz numer telefonu do kontaktu w sprawie. W tym samym dniu powódka otrzymała za pośrednictwem komunikatora (...) wiadomość od osoby oznaczonej jako (...), że chce on nabyć wystawiony przedmiot. (...) korzystał z numeru telefonu (...). W trakcie rozmowy za pomocą (...) nabywca był zainteresowany zakupem bluzy, zadawał pytania. Ostatecznie zdecydował się na jej zakup i poinformował powódkę o możliwości wysyłki bluzy poprzez (...). Przesłał powódce za pomocą komunikatora (...) link (...) M. B. odpowiedziała, że nie zaznaczyła opcji wysyłki przez (...), ale jeśli będzie możliwość dokonania zmiany tej opcji, to z niej skorzysta. Powódka zmieniła opcje dostawy towaru przez (...) na portalu (...) i poinformowała kupującego, że w dniu następnym wysyła bluzę. (...) wyjaśnił również w wiadomości, że zapłacił za towar i dostawę oraz podał, że otrzyma ona pieniądze za pomocą powyższego linku. Przesłał jej zdjęcie potwierdzenia zapłaty. Powódka skorzystała z linku przesłanego przez (...), celem odbioru pieniędzy. Link wykorzystywał wizerunek (...) i przekierował ją do bankowości internetowej celem odebrania pieniędzy za sprzedany towar. M. B. była przekonana, że korzysta z usług operatora (...) oraz strony internetowej pozwanego banku. W rzeczywistości było to łącze do fikcyjnego serwisu (...) i płatności. Powódka podała dane logowania. Hasło również zostało pozyskane przez nieznane osoby. Po otrzymaniu tych danych nieznane osoby zalogowały się do rachunku bankowego powódki w bankowości internetowej. Następnie M. B. w tym samym dniu o godz. 12.48 i 12.51 otrzymała smsy z Banku z kodami do autoryzacji, które wpisała do formularza na fikcyjnej stronie, a z nich skorzystała nieznana osoba. Nieznana osoba w dniu 30 marca 2021 r. między godz. 12.48 a 12.51 zdefiniowała kod PIN oraz dodała swoje urządzenie mobilne (...). Mogła już samodzielnie dokonywać autoryzacji transakcji na rachunku bankowym powódki.

(Dowód: opinia biegłego 229-235, wydruk ekranu komputera powódki k. 58, wydruk korespondencji z (...) k. 49, 50, 51, 52, 53, 54, 58, zapis rozmowy telefonicznej powódki z pracownikiem banku k. 218-223, smsy z kodami k. 46-47, zeznania W. M. k. 207v-209)

W dniu 30 marca 2021 r. miały miejsce transakcje bankowe, których nie zlecała M. B.. Były to następujące przelewy z dnia 30 marca 2021 r. :

1. z rachunku o nr (...) należącego do powódki na rachunek o nr (...) należący do nieznanego powódce odbiorcy o danych A. M. S. na kwotę 31.691,00 zł,

2. z rachunku o nr (...) należącego do powódki na rachunek powódki o nr (...) na kwotę 12.689,00 zł,

3. z rachunku o nr (...) należącego do powódki i jej męża P. B. na rachunek powódki o nr (...) na kwotę 11.111,00 zł,

4. z rachunku o nr (...) należącego do matki powódki T. K. na rachunek powódki o nr (...) na kwotę 3.050,00 zł,

5. z rachunku o nr (...) należącego do matki powódki T. K. na rachunek powódki o nr (...) na kwotę 3.050,00 zł,

6. z rachunku o nr (...) należącego do brata powódki D. K., na rachunek powódki o nr (...) na kwotę 2.700,00 zł.

(Dowód: potwierdzenie transakcji k. 40-45, historia transakcji k. 122, zapis rozmowy powódki z pracownikiem banku k. 218-223)

Pozwany monitoruje transakcje płatnicze pod kątem oceny ich ryzyka. O godz. 12.52 powódka otrzymała od pozwanego sms'a z informacją, że tymczasowo zablokowano jej bankowość internetową z uwagi na podejrzane logowanie.

(Dowód: treść sms'a k. 48, zapis rozmowy powódki z pracownikiem banku k. 218-223, zeznania W. M. k. 207v-209)

Portal (...)oferował usługę (...) Była to usługa uruchomiona przez operatora dla osób, które chciały sprzedać towar w ramach portalu. Polegała na możliwości nadania przesyłki w Urzędzie Pocztowym lub paczkomacie InPost. Jednocześnie usługa wymagała podania danych bankowych w celu odebrania zapłaty za sprzedany przedmiot.

(Dowód: wydruk ze strony internetowej (...) k. 55-57)

Pismem z dnia 15 kwietnia 2021 r. pozwany nie uwzględnił reklamacji powódki i nie zwrócił jej kwoty 33.691,00 zł. Powódka pismem z dnia 26 kwietnia 2021 r. wezwała pozwanego do zwrotu tej kwoty do dnia 05 maja 2021 r. Pozwany bank pismem z dnia 04 maja 2021r. podtrzymał swoje poprzednie stanowisko.

(Dowód: pismo pozwanego k. 38-39, pismo powódki k. 67, pismo pozwanego k 68-70)

Na podstawie zawiadomienia dokonanego przez A. B. Komenda Miejska Policji w K. wszczęła w dniu 07 maja 2021 r. dochodzenie o przestępstwo oszustwa komputerowego, określonego w art. 287 § 1 k.k.

(Dowód: pismo KMP w K. k. 66)

Logowanie w dniu 30 marca 2021 r. o godzinie 12.48-12.51.52, na rachunek bankowy powódki i powiązane z nim rachunki, w wyniku których doszło następnie do nieautoryzowanych przez powódkę przelewów, nastąpiło z innego urządzenia niż powódki. Do zdarzenia doszło w wyniku tzw. phishingu. Jest to forma oszustwa, polegająca na podszyciu się przez przestępców pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji typu np. dane do logowania lub dane karty kredytowej, bądź też zainfekowania komputera szkodliwym oprogramowaniem. W dniu 30 marca 2021 r. powódka padła ofiarą takich działań, gdyż nieznana osoba przy pomocy fałszywej strony internetowej (...) i pozwanego banku uzyskała login i hasło do jej bankowości elektronicznej poprzez podszycie się pod serwis

internetowy platformy sprzedażowej oraz pozwanego banku. Powódka uznała, że jest na prawdziwej stronie (...). oraz pozwanego. Kliknęła więc w link prowadzący do systemu płatności celem otrzymania zapłaty od (...). Dopiero sms z Banku o blokadzie pozwolił powódce ustalić, że ktoś wykonuje z jej konta jakieś transakcje. Kolejne przelewy, które odbyły się bez wiedzy powódki, były nieautoryzowane, w wyniku wprowadzenia rzeczonego zaufanego odbiorcy. Z punktu widzenia systemu bankowego pozwanego banku nieautoryzowane transakcje na łączną kwotę 33.691,00 zł zostały zlecone przez powódkę.

Logowanie do serwisu internetowego pozwanego banku odbywa się poprzez podanie loginu i hasła, dodatkowo wyświetla się obrazek bezpieczeństwa. W przypadku powódki, powódka autoryzowała czynności kodem sms, w zakresie zmiany kodu PIN (k. 123) i dodania urządzenia mobilnego, które podawała nieznanym osobom. Nie wyświetlała jej się informacja, że dokonywane są na jej rachunku bankowym jakieś transakcje płatnicze, które to czynności wymagały autoryzacji sms-kodem. Autoryzacji przelewów bankowych dokonywała kodem sms nieznana osoba po dodaniu swego telefonu jako urządzenia zaufanego.

Nie ujawniono niepożądanych zachowań aplikacji, smartfona czy komputera obsługiwanych przez powódkę. Żadne z tych urządzeń nie przyczyniło się do samoczynnej autoryzacji oszustwa. Posiadanie aktualnego oprogramowania antywirusowego, zapory sieciowej, przeglądarki internetowej nie uchroniłaby M. B. przed atakiem phishingowym. Nikt nie włamał się na telefon powódki i zdalnie z jej telefonu nic nie robił. Powódka nieświadomie przekazywała sms'y z kodami i autoryzowała aplikację banku (...) na urządzeniu osoby trzeciej. Nie doszło też do złamania przez osobę trzecią zabezpieczeń na stronie bankowości elektronicznej pozwanego.

(Dowód: opinia biegłego k. 229-235, uzupełniająca opinia biegłego k. 259-263, historia transakcji k.122, treść sms'ow k. 123, geolokalizacja adresów IP k. 169, 170, zeznania W. M. k. 207v-209)

Pozwany w okresie od 03 września 2019 r. do 15 czerwca 2021 r. zamieszczał na stronie internetowej informacje o możliwych sposobach oszustw.

(Dowód: wydruk ze strony internetowej pozwanego k. 164-168, 190-196)

Powyższy stan faktyczny Sąd ustalił na podstawie wskazanych powyżej dokumentów, które Sąd w całości uznał za wiarygodne, gdyż ich rzetelność i prawdziwość nie była przez strony kwestionowana oraz w oparciu o okoliczności między stronami bezsporne.

Za wiarygodne Sąd uznał zeznania świadka W. M., pracownika pozwanego banku. Sąd wziął pod uwagę wiedzę świadka o procedurach obowiązujących w banku oraz okoliczności zlecenia nieautoryzowanych przelewów, będące przedmiotem sporu i w tym zakresie Sąd dał wiarę świadkowi w całości.

Sąd dał wiarę również opinii biegłego sądowego z zakresu informatyki M. D.. Sąd dokonując oceny tej opinii miał na uwadze wysoki poziom wiedzy biegłego, podstawy teoretyczne opinii, sposób motywowania sformułowanego stanowiska, stopień stanowczości wyrażonych w niej ocen, zgodność z zasadami logiki i wiedzy powszechnej. Biegły w sposób logiczny i jasny przedstawił tok rozumowania prowadzący do sformułowanych w opinii wniosków, a jego opinia jest zrozumiała i kompletna. Biegły w opinii uzupełniającej zweryfikował zarzuty pozwanego i obronił wnioski zawarte w opinii.

Sąd zważył co następuje:

Zdaniem Sądu powództwo zasługiwało na uwzględnienie.

W ocenie sądu istotnym było ustalenie, czy w niniejszej sprawie niedbalstwo po stronie powodowej miało cechy rażącego niedbalstwa, jako kwalifikowanej formy winy czy cechy „zwykłego" niedbalstwa, o czym decydowało ustalenie wzorca staranności, wymaganego w stosunkach danego rodzaju.

Na uwagę zasługuje wyrok z dnia 24 maja 2018 r. Sądu Apelacyjnego w Warszawie w sprawie sygn. akt VI ACa 217/17 w którym to wyroku Sąd wskazał, że „jeśli transakcje zostały zrealizowane bez zgody płatnika oraz w okolicznościach, za które nie ponosi on odpowiedzialności, a następnie płatnik dokonał zgłoszenia wystąpienia nieautoryzowanych transakcji, to na dostawcy ciąży obowiązek zwrotu 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 z 2011 r. o usługach płatniczych), wówczas to on, a nie dostawca odpowiada za nieautoryzowane transakcje".

Zgodnie z treścią art. 355 § 1 k.c., dłużnik obowiązany jest do staranności ogólnie wymaganej w stosunkach danego rodzaju (należyta staranność).

Sąd wskazuje, iż co do zasady 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 (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 08 lipca 1998 r., III CKN 574/97).

Pojęcie należytej staranności jest miernikiem 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 2007r., sygn. akt II CSK 170/07, por. też wyrok Sądu Najwyższego z dnia 10 marca 2004r., sygn. akt IV CK 151/03).

W ocenie Sądu art. 355 k.c. kładzie wyraźny akcent na rodzaj stosunków, przez co należy rozumieć rodzaj przedsięwziętej aktywności, przy czym uwzględniając rodzaj działalności, należy zważyć, że chodzi o miarę staranności powszechnie przyjętą, do pewnego stopnia obiektywną, wynikającą z nakazów sztuki, umiejętności lub techniki, którą można w konkretnym przypadku ustalić, stosując uchwytne mierniki staranności. Ocena stopnia staranności nie może być dowolna, musi poddawać się weryfikacji (wyrok sądu Najwyższego z dnia 21 września 2007 r., sygn. akt V CSK 178/07).

Sąd nie podzielił stanowiska strony pozwanej co do okoliczności, że to po stronie powodowej doszło do rażącego niedbalstwa.

Owszem, nie doszło do złamania zabezpieczeń systemu bankowego, bowiem sama powódka ujawniła osobom nieuprawnionym swoje poufne dane, a więc login, hasło, sms-kod - na fałszywej stronie, umożliwiając w ten sposób sprawcom przestępstwa ich przejęcie, a następnie wykorzystanie bez jej wiedzy. Jednak uczyniła to nieświadomie, w wyniku sprawnego działania oszustów, którzy korzystając z ludzkiej nieświadomości, naiwności, pośpiechu, a także innych czynników osłabiających czujność klienta dokonywali tego rodzaju przestępstw, przy korzystaniu przez takie osoby z usług bankowości elektronicznej.

Nie sposób jednak zgodzić się ze stanowiskiem pozwanego o przyjęciu rażącego niedbalstwa po stronie powódki, jako przyczyny zwalniającej pozwany bank z odpowiedzialności. W ocenie Sądu nie są oczywiste okoliczności, że stale i nieprzerwanie widniały na stronie internetowej pozwanego ostrzeżenia dotyczące zachowania należytego bezpieczeństwa podczas logowania do bankowości mobilnej banku, a powódka mogła się z nimi z łatwością zapoznać. Oczywiście rynek usług bankowości elektronicznej stale się rozwija i świadomość jego klientów na dzień dzisiejszy z pewnością jest większa, jednak Sąd nie podziela przekonania, że metody działania hakerów i środki obrony przed nimi były powszechnie znane.

Odnieść należy się do ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. z 2022 r. poz. 2360, dalej u.u.p.). Zgodnie z art. 46 ust 3 tej ustawy, 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 ustawy. Podobny zapis znalazł się w § 34 ust. 3 regulaminu świadczenia usług bankowości elektronicznej pozwanego banku.

Wskazana ustawa stanowi akt prawny, który w sposób kompleksowy reguluje rynek usług płatniczych-określa zarówno 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 (por. Barbara Bajor, Jan Brylski, Anna Zalcewicz, Ustawa o usługach płatniczych. Komentarz, wyd. II. LEX 2017). Stosownie do postanowień art. 1 ustawa określa zasady świadczenia usług płatniczych oraz wydawania i wykupu pieniądza elektronicznego. Zwrócić należy uwagę, że ustawa w swojej treści zawiera rozwiązania prawne zarówno natury prywatnoprawnej, jak i publicznoprawnej. W ustawie określone zostały warunki świadczenia usług płatniczych, w szczególności wymogi dotyczące obowiązków informacyjnych dostawców usług płatniczych w przypadku zawierania umów ramowych oraz w odniesieniu do każdej pojedynczej usługi płatniczej. Uregulowane zostały również zasady, których zasadniczym celem jest zwiększenie przejrzystości postanowień umów o świadczenie usług płatniczych i w sposób jasny oraz zrozumiały określenie praw i obowiązków stron umowy, w tym w szczególności rodzajów i wysokości pobieranych opłat z tytułu świadczonej usługi. W ten sposób został podkreślony prokonsumencki charakter rozwiązań ustawy.

W art. 2 ww. ustawy zamieszczono tzw. słownik zawierający objaśnienia określeń ustawowych, co pozwala na identyfikację stron stosunku prawnego – powódki jako płatnika oraz strony pozwanej jako dostawcę usługi. Przez usługi płatnicze ustawa rozumie działalność polegającą między innymi na wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub innego dostawcy przez wykonywanie usług polecenia przelewu. Działalność w zakresie świadczenia usług płatniczych może być wykonywana wyłącznie przez dostawców usług płatniczych, którymi mogą być podmioty wymienione w ustawie, m.in. bank krajowy w rozumieniu art. 4 ust. 1 pkt 1 ustawy Prawo bankowe.

Rozdział 2 (art. 40 i n.) działu III ustawy poświęcony został problematyce autoryzacji transakcji płatniczych, skutków braku autoryzacji transakcji oraz zasad i zakresu odpowiedzialności dostawcy i płatnika za transakcje nieautoryzowane, jak też nienależycie wykonane czy niewykonane. 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. wpisaniu kodu z sms'a, przez użycie kolejnego kodu z karty kodów). Prawidłowa, zgodna z określonymi w załączonych do umowy 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 u.u.p., 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.

Przyjęte rozwiązanie sugeruje, że płatnik, zlecając wykonanie transakcji płatniczej, czyli składając oświadczenie woli, musi autoryzować transakcję. Oznacza to, że samo złożenie oświadczenia woli, na mocy którego płatnik zleca wykonanie transakcji, nie jest wystarczające - nie jest równoznaczne z wyrażeniem zgody.

W art. 42 ustawy 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 treścią 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.

Artykuł 45 ustawy zawiera szczególną regułę dotyczącą ciężaru dowodu w przypadku dochodzenia roszczeń z tytułu nieautoryzowanych, nienależycie wykonanych lub niewykonanych transakcji. 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 chce wywodzić skutki prawne dla siebie. Oznaczałoby to, że jeśli użytkownik kwestionuje fakt autoryzowania transakcji przez siebie, musiałby to wykazać. Rozwiązania przyjęte w omawianej ustawie przerzucają ciężar udowodnienia na dostawcę. Stanowią one wyraz prokonsumenckiego charakteru ustawy. Ciężar udowodnienia, że transakcja była autoryzowana przez użytkownika, ciąży na dostawcy, czyli na profesjonaliście, 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. Jednak dostawca musi przywołać inne dowody niż sam fakt prawidłowego skorzystania z procedur autoryzacji przewidzianych umową. Dostawca może przytoczyć dowody wykazujące, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji (np. przekazał kartę i PIN członkowi rodziny) albo wskutek rażącego niedbalstwa naruszył jeden z obowiązków określonych w art. 42 u.u.p., czyli nie przechowywał informacji w sposób zapewniający bezpieczeństwo.

Zasady odpowiedzialności dostawcy oraz płatnika w przypadku wystąpienia nieautoryzowanych transakcji ustawodawca ustala w art. 46 ustawy. W świetle ust. 1 powołanego przepisu,w przypadku wystąpienia nieautoryzowanych transakcji dostawca jest zobowiązany do zwrotu płatnikowi kwoty nieautoryzowanej transakcji niezwłocznie. 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 u.u.p.), 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.

Zobowiązanie banku jako profesjonalnego podmiotu jest determinowane poprzez ustawowe obowiązki wskazane m.in. w art. 43 ust. 1 u.p.p. Pozwany bank nie wywiązał się z ich wypełnienia w stosunku do powódki. W szczególności nie zapewnił, by indywidualne zabezpieczenia instrumentu płatniczego nie były dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Gdyby bowiem zabezpieczenia transakcji elektronicznych stosowane przez pozwanego były właściwe, nie doszłoby do dokonania na rachunku powódki transakcji przez nieuprawnione do tego osoby.

M. B. jako klient banku nie naruszyła obowiązków, o których mowa w art. 46 ust. 3 u.p.p., umyślnie lub wskutek rażącego niedbalstwa. Z pewnością działanie powódki nie było umyślne, powódka uważała, że działa na platformie (...), tym bardziej, że (...) świadczy taką usługę jak przesyłka. Nadto powódka nie zlecała przelewów kwot, co mogłoby ją zastanawiać i szybciej uświadomić, że są jakieś niepożądane transakcje płatnicze. Powódka chciała jedynie z systemu (...) odebrać pieniądze za sprzedaną bluzę. Mogły zatem nie wzbudzić jej podejrzeń kody autoryzacyjne skoro nie dotyczyły płatności. Zdaniem Sądu powódce nie można również przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa. M. B. nie udostępniała świadomie loginu, hasła ani innych danych jakimkolwiek osobom trzecim. W dniu 30 marca 2021 r. powódka wykonywała pewne czynności w systemie bankowości internetowej, jednak dokonanie przelewów na łączną kwotę 33.691,00 zł z rachunków bankowych nastąpiło poza jej wiedzą i bez autoryzacji. Oszust uzyskał login i hasło do jej bankowości elektronicznej poprzez podszycie się pod serwis internetowy (...) i pozwanego banku. Doszło wprawdzie do potwierdzenia transakcji za pomocą właściwego narzędzia, jednak wykonanie kolejnych przelewów nastąpiło bez wyrażenia zgody przez powódkę na ich dokonanie. Powódka autoryzowała PIN oraz dodała urządzenie mobilne, które to czynności wymagały autoryzacji sms-kodem. W pierwszym sms-ie widniała informacja, że jest to autoryzacja PIN, a w drugim sms-ie była podana informacja o autoryzacji dla urządzenia (...). Kolejne przelewy, które odbyły się bez wiedzy powódki, były nieautoryzowane, w wyniku wprowadzenia rzeczonego urządzenia. Jest niewątpliwie uchybieniem po stronie powódki, że niezbyt precyzyjnie weryfikowała komunikaty na ekranie telefonu, w pewnym zakresie z pewnością działaniu powódki można postawić zarzut nienależytej staranności, jednakże nie w stopniu rażącym. Należy zgodzić się z twierdzeniem biegłego wyrażonym w opinii, którą Sąd uznał za wiarygodną, iż w sytuacji stresowej i poddana manipulacji powódka zapomniała o wszystkim o czym powinna pamiętać. Z drugiej jednak strony trzeba wziąć pod uwagę profesjonalizm przestępstwa – sprawcę trudno wykryć. Jednocześnie wiedza odnośnie różnic w wyglądzie strony banku i strony fałszywej jest wiedzą, którą dysponuje profesjonalista, ale nie jest powszechnie dostępna zwykłemu użytkownikowi, który zazwyczaj nie zwraca uwagi na istotne detale. Uchybienia powódki, które zaistniały nie mogą być kwalifikowane jako rażące niedbalstwo. Stosownie do art. 50 ust. 2 ustawy prawo bankowe (Dz.U. z 2022 r. poz. 2324) na bankach ciąży powinność dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Trudno było uznać jako w pełni odpowiadające tym wymogom działanie polegające na braku odpowiedniej reakcji na dokonywane na rachunku powódki i na tych do których miała pełnomocnictwo operacje bankowe dotyczące przelewów w krótkim czasie.

Mając powyższe na uwadze Sąd orzekł jak w punkcie 1 i 2 wyroku. Sąd oddalił częściowo powództwo w zakresie odsetek od dnia 31 marca 2021 r. Sąd przyjął, iż pozwany jest zobowiązany do zapłaty odsetek w myśl art. 481 k.c. w zw. z art. 455 k.c. W myśl powołanego przepisu, jeżeli termin spełnienia świadczenia nie jest oznaczony ani nie wynika z właściwości zobowiązania, świadczenie powinno być spełnione niezwłocznie po wezwaniu dłużnika do wykonania. Do czasu wezwania pozwanego przez powódkę i wyznaczenia terminu pozwany nie był zobowiązany do zwrotu. M. B. wezwała pozwanego do zapłaty pismem z dnia 26 kwietnia 2021 r. i wyznaczyła termin do dnia 05 maja 2021 r. Pozwany odmówił powódce zwrotu kwoty w dniu 04 maja 2021 r., a zatem od dnia następnego czyli 05 maja 2021 r. był już w opóźnieniu ze spełnieniem świadczenia.

O kosztach procesu orzeczono zgodnie z zasadą wyrażoną w art. 98 § 1 i 3 k.p.c. nakładając na pozwanego, jako stronę przegrywającą postępowanie, obowiązek zwrotu wszystkich poniesionych w sprawie przez powódkę kosztów.

Izabela Ozdowska-Chojnacka