Sygn. akt V Ga 328/21

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 28 stycznia 2022 r.

Sąd Okręgowy w Olsztynie, V Wydział Gospodarczy, w składzie:

Przewodniczący: sędzia Iwona Nowak

Protokolant: st. sekr. sąd. Joanna Kotowska

po rozpoznaniu w dniu 12 stycznia 2022 r. w Olsztynie

na rozprawie

sprawy z powództwa J. O.

przeciwko (...) Bank (...) S.A. z siedzibą w W.

o zapłatę

na skutek apelacji pozwanego od wyroku Sądu Rejonowego w Olsztynie
z dnia 16 września 2021 r., sygn. akt V GC 1152/20

I. Oddala apelację

II. Zasądza od pozwanego na rzecz powoda kwotę 1800 złotych (słownie : jeden tysiąc osiemset złotych)tytułem zwrotu kosztów instancji odwoławczej z odsetkami w wysokości odsetek ustawowych za opóźnienie w spełnieniu świadczenia pieniężnego za czas od dnia uprawomocnienia się niniejszego orzeczenia w przedmiocie kosztów procesu do dnia zapłaty

Sędzia Iwona Nowak

Sygn. Akt V Ga 328/21

UZASADNIENIE

Pozwem z dnia 15 maja 2020 roku (data stempla pocztowego) powód J. O. wniósł o zasądzenie od pozwanego (...) Bank (...) S.A. z siedzibą w W. kwoty 29.764,99 złotych wraz z odsetkami ustawowymi za opóźnienie od dnia 28 lutego 2019 roku do dnia zapłaty. Nadto wniósł o zasądzenie zwrotu kosztów procesu, w tym zwrotu kosztów zastępstwa procesowego według norm przepisanych, wraz z odsetkami ustawowymi za opóźnienie od dnia uprawomocnienia się orzeczenia do dnia zapłaty.

W uzasadnieniu swojego roszczenia wskazał iż w dniu 20 listopada 2018 roku za pośrednictwem sieci Internet doszło do przełamania informatycznych zabezpieczeń internetowego serwisu transakcyjnego pozwanego , a następnie dokonania nieautoryzowanej transakcji przelewu internetowego na kwotę dochodzoną niniejszym pozwem. Jako podstawę dochodzone roszczenia powód powołał art 471 k.c.

W odpowiedzi na pozew pozwany (...) Bank (...) S.A. z siedzibą w W. wniósł o oddalenie powództwa w całości oraz zasądzenie od powoda na rzecz pozwanego zwrotu kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych.

W uzasadnieniu wskazano, że przy dokonywaniu spornych transakcji na rachunku powódki nie doszło do złamania zabezpieczeń systemów bankowych, zalogowanie nastąpiło z podaniem prawidłowego loginu powódki, zaś same transakcje zostały zrealizowane w oparciu o szablon płatności prawidłowo aktywowany przy pomocy jednorazowego kodu aktywacyjnego przekazanego drogą wiadomości SMS na numer telefon powódki. Nie można wobec tego mówić w niniejszej sprawie o nieautoryzowanej transakcji w rozumieniu art. 40 ustawy- o transakcjach płatniczych. Dodatkowo zarzucił powodowi brak zachowania terminu niezwłocznego zawiadomienia pozwanego banku o zaistniałym zdarzeniu.

Wyrokiem z dnia 16 września 2021 r. Sąd Rejonowy w Olsztynie w sprawie V GC 1152/20 :

I. zasądza od pozwanego (...) Bank (...) S.A. z siedzibą w W. na rzecz powoda J. O. kwotę 29.764,99 złotych wraz z odsetkami ustawowymi za opóźnienie od dnia 28 lutego 2019 roku do dnia zapłaty

II. zasądza od pozwanego na rzecz powoda kwotę 5106 złotych tytułem zwrotu kosztów procesu z ustawowymi odsetkami za opóźnienie od dnia uprawomocnienia się wyroku do dnia zapłaty

W pisemnym uzasadnieniu wyroku Sąd Rejonowy wskazał na następujące ustalenia i motywy swojego rozstrzygnięcia.

W dniu 15 listopada 2014 roku powód prowadzący działalność gospodarczą pod firmą Firma Handlowo- Usługowa (...) J. O. zawarł z pozwanym (ówcześnie Bank (...) S.A. z siedzibą we W.) umowę usług bankowości elektronicznej (...) M. Firma , w której został określony numer NIK klienta , numer telefonu do autoryzacji SMS kodu .Załącznik do umowy regulował zasady korzystania z usług bankowości elektronicznej . Strony w dniu 26 sierpnia 2016 roku zawarły aneks do umowy w rachunku bieżącym.

Zgodnie z rozdziałem (...) Zasad korzystania z usług bankowości elektronicznej – identyfikacja użytkownika polega na prawidłowym podaniu numeru(...) i hasła (...). Ponadto złożenie dyspozycji przez klienta polega na podaniu danych wskazanych w ust(...) niniejszego paragrafu , dokonaniu autoryzacji i wysłaniu dyspozycji do banku. O ile inne regulacje wiążące klienta z bankiem nie stanowią inaczej , podstawą realizacji transakcji , będzie wyłącznie unikatowy identyfikator podany przez klienta , którym jest:

a) w przypadku Przelewu – numer rachunku bankowego podany w formacie akceptowanym przez Bank ((...) , (...))

b) w przypadku Przelewu w celu zasilenia kont bez abonamentowych telefonów komórkowych – numer telefonu komórkowego

c) w przypadku Przelewu (...) składanego w usłudze (...) wersja aplikacyjna – nazwa sklepu

Ustawienie parametrów usług (...) dokonane jest przez klienta w ramach usługi (...) i jest wiążące dla klienta.

W przypadku (...) , którego kwota nie przekracza wysokości dziennego limitu przelewów na rachunki obce dla transakcji nie zabezpieczonych tokenem lub sms Kodem autoryzacja następuje poprzez wybranie na ekranie odpowiedniego przycisku. Niezależnie od powyższego w zakresie (...), Bank bez względu na kwotę może wymagać również podania odpowiedniego jednorazowego kodu generowanego przez token lub sms Kodu przesłanego na telefon komórkowy .

Zgodnie z § 17 Klient powinien się upewnić ,że wszelkie dyspozycje składane w ramach usług (...) są jednoznaczne i zgodne z jego intencją , zawierają prawidłowo wskazane dane , a ponadto określają rachunki , która mają być obciążane/uznawane , właściciela tych rachunków oraz tytuł płatności.

W dniu 20 listopada 2018 roku córka powoda a zarazem pracownik powodowej firmy wykonywała przelewy bankowe dla kontrahentów . Transakcje były dodawane do koszyka przelewów, który umożliwiał dokonanie kilku przelewów w jednym czasie. Do koszyka został dodany cykliczny przelew należności za paliwo do zdefiniowanego odbiorcy –stacja

paliw (...) sp. z o.o.. Dyspozycja została potwierdzona SMS kodem . Zgodnie z SMS Kodem dyspozycja opiewała na kwotę 29.764,99 złotych i miała być skierowana do odbiorcy Stacji Paliw (...) sp. z o.o.

W konsekwencji z rachunku powoda został wykonany przelew na powyższą kwotę na rachunek bankowy E. M. nr (...). Tego samego dnia z rachunku E. M. została dokonana wypłata gotówki w kwocie 20.000 złotych oraz został wykonany przelew na rachunek B. C. nr (...). W wyniku działań E. M. środki zostały rozdzielone i częściowo wpłacone na „ wirtualny portfel ” waluty B. , a częściowo przekazane dalej do B. C..

Z uwagi na fakt iż firma (...) sp. z .o. nie odnotowania wpłaty należności za paliwo , przedstawiciel w dniu 26 lutego 2019 roku poinformował o powyższym fakcie powoda. Powód poinformował pozwanego natychmiast.

W dniu 11 marca 2019 roku pozwany poinformował powoda o nie stwierdzonych nieprawidłowościach po stronie banku. Płatność bowiem została wykonana z koszyka i zatwierdzona sms kodem wysłanym na numer telefonu, zgodnie z dyspozycją oraz przekazana na wskazany numer rachunku. Wskazano ,że bank informował klientów o istnieniu zagrożenia w sieci Internet w drodze komunikatów umieszczanych po zalogowaniu się do usług bankowości elektronicznej , m.in. pouczając jak postępować. Ponadto ustalono ,że system bankowy nigdy nie zanotował modyfikacji danych odbiorcy zdefiniowanego jako firma (...) sp. z o.o. w bankowości elektronicznej powoda .

Analiza logów bankowych wykazała ,i w trakcie definiowania nowego przelewu , poprawne dane stacji paliw (...) sp. z o.o. zostały pobrane z systemu bankowości elektronicznej, natomiast chwilę po tej operacji , zostały podmienione na dane E. M.. Powód nie mógł sam wprowadzić tych danych w formatkę przelewu bowiem system blokował możliwość edycji danych dla odbiorcy zdefiniowanego.

Sporna transakcja została wykonana przez wykorzystanie szkodliwego oprogramowania typu „ malware ”, które musiało funkcjonować na komputerze powoda w dniu 20 listopada 2018 roku. W procesie autoryzacji spornej dyspozycji nie wystąpiły naruszenia bezpieczeństwa systemu bankowego, gdyż atak na rachunek bankowy powoda został przeprowadzony przy użyciu komputera poszkodowanego – powoda.

Powyższy stan faktyczny Sąd Rejonowy ustalił na podstawie dokumentów złożonych do akt jak i z dokumentów z akt dochodzenia (...), 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 Rejonowy uznał zeznania świadków zawnioskowanych przez strony, które to były spójne i korelowały ze sobą.

Kluczowym dla Sądu pierwszej instancji była przede wszystkim opinia biegłego z zakresu ochrony praw autorskich , oprogramowania komputerowego , elektronicznych systemów bankowych , baz danych i sieci komputerowych sporządzona przez M. W..

Zdaniem Sądu Rejonowego powództwo zasługiwało na uwzględnienie w całości .

Na wstępie rozważań Sąd Rejonowy powołał się na art. 725 k.c. wskazując iż między stronami doszło do zawarcia umowy rachunku bankowego w wyniku , której bank nabywa własność wniesionych środków pieniężnych , a posiadacz rachunku bankowego nabywa roszczenie o zwrot sumy pieniężnej wynikającej z postanowień umowy łączącej klienta z bankiem. Oznacza to jak stwierdził m.in. Sąd Apelacyjny w Krakowie w wyroku z dnia 5 lutego 2014 r na którego to wyrok powołał się sąd ,że wszelkie operacje dokonywane na rachunku bankowym wbrew woli posiadacza rachunku nie obciążają tego posiadacza , a jedynie bank.

Sąd za biegłym uznał iż sporna transakcja została wykonana przez działanie szkodliwego oprogramowania typu „ malware” , które to musiało funkcjonować na koncie powoda w dniu 20 listopada 2018 roku.. Analiza logów bankowych przeprowadzona przez biegłego wykazał ,że w trakcie definiowania nowego przelewu , poprawne dane stacji paliw (...) sp. z o. o . zostały pobrane z systemu bankowości elektronicznej , natomiast chwilę później zostały podmienione na dane E. M.. Powód nie mógł fizycznie sam wprowadzić tych danych w formatkę przelewu , ponieważ

pozwany blokował możliwość edycji danych dla odbiorcy zdefiniowanego , a sam system bankowy dotychczas nie zanotował modyfikacji danych odbiorcy zdefiniowanego jako (...) sp. z o.o. w bankowości

Sąd I instancji przywołał również wyrok z dnia 19 lipca 2018 Sądu Apelacyjnego w Warszawie w którym to wyroku Sąd wskazał, że "podstawą odpowiedzialności banku w tym zakresie stanowią normy prawne zawarte w ustawie a dnia 19 sierpnia 2011 roku o usługach płatniczych" . Powołana ustawa przewiduje generalną zasadę , zgodnie z którą dostawca usług płatniczych czyli bank , ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika czyli posiadacza konta.

Zgodnie z art. 46 ust 1 wyżej cytowanej ustawy w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie , nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika lub po dniu otrzymania stosownego zgłoszenia zwrócić płatnikowi kwotę nieautoryzowanej transakcji , 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 ściągania przestępstw.

W przypadku gdy płatnik korzysta z rachunku płatniczego , dostawca płatnika przywraca obciążony rachunek płatniczy do stanu , jaki istniałby , gdyby nie miała miejsce nieautoryzowana transakcja płatnicza. Przy czym w art. 45 ust 1 wyżej cytowanej ustawy wskazano ,że ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika 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 spoczywa na dostawcy tego użytkownika – czyli na pozwanym.

Zatem pozwany odpowiada za nieautoryzowane transakcje płatnicze.

Dodatkowo Sąd pierwszej instancji wskazał ,ze zobowiązanie pozwanego względem powoda jako posiadacza rachunku wynika z art. 50 ust 2 ustawy z dnia 29 sierpnia 1997 roku -Prawo bankowe (tekst jedn.:Dz. Us. z 2012 poz. 1376 z późn. zm.) ,który to stanowi ,że bank jest zobowiązany do dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych . W ocenie Sądu pierwszej instancji pozwany nie dołożył należytej staranności w tym zakresie i w związku z powyższym ponosi odpowiedzialność na podstawie art. 471 k.c i zgodnie z art. 46 ust 1 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych jest zobowiązany niezwłocznie zwrócić powodowi kwotę nieautoryzowanej transakcji handlowej w kwocie 29.764,99 złotych.

Od powyższego wyroku apelację wniósł pozwany, zaskarżając przedmiotowe orzeczenie w całości

Wyrokowi temu skarżący zarzucił naruszenie:

1.przepisów postępowania, a mianowicie art. 233 k.p.c. poprzez przekroczenie zasady swobody oceny dowodów i dokonanie ustaleń faktycznych z pominięciem zasad logiki i doświadczenia życiowego poprzez:

a. przyjęcie ,że powód –pomimo upływu 4 miesięcy od chwili transakcji do chwili jej dostrzeżenia- nie dopuścił się rażącego niedbalstwa,

b. nieuwzględnienie w ocenie stanu faktycznego sprawy faktu , że powód nie posiadał wymaganych zabezpieczeń urządzeń z których korzystał do obsługi bankowości elektronicznej i – na skutek własnych zaniedbań – dopuścił do zainstalowania oprogramowania śledzącego,

c. nieuwzględnienie w ocenie stanu faktycznego sprawy faktu ,że powód był przez pozwanego ostrzegany o istniejących ryzykach oraz informowany o potencjalnych sposobach działania przestępców , a mimo posiadania tej wiedzy nie dochował staranności w ochronie dostępu do swoich rachunków bankowych.

2.prawa materialnego tj art. 46 ustawy o usługach płatniczych oraz art. 40 ustawy o usługach płatniczych poprzez błędną wykładnię i błędne przyjęcie ,że na mocy ww. przepisu pozwany ponosi właściwie niczym nieograniczoną odpowiedzialność za środki finansowe zgromadzone przez powoda , w tym nawet w sytuacji rażącego niedbalstwa powoda polegającego na dokonaniu autoryzacji transakcji , dopuszczeniu do instalacji złośliwego oprogramowania szpiegowskiego i niedostrzeżeniu rzekomego braku autoryzacji przez okres 4 miesięcy.

W petitum apelacji, pozwany przedstawił treść wymienionych zarzutów, obszernie wskazując w czym konkretnie upatruje naruszenia wskazanych regulacji. Tezy te autor apelacji rozwinął w uzasadnieniu wniesionego środka odwoławczego wskazując na fakt ,iż do autoryzacji spornych dyspozycji doszło na skutek działań powoda. Między innymi z powodu zaniedbań w zabezpieczeniu sprzętu na którym to powód prowadził obsługę bankowości elektronicznej oraz z uwagi na fakt poinformowania pozwanego o zaistniałej sytuacji blisko po upływie 4 miesięcy. Wskazał ,że powód miał informację o ryzyku związanym z tzw. (...). O braku obowiązku zwrotu kwoty kwestionowanej przez powoda świadczy wprowadzenie przez ustawodawcę zapisu treści art. 46 ust 2-3 ustawy o środkach płatniczych. Pozwany powołał się brzmienie motywu (70)do Dyrektywy Parlamentu Europejskiego i Rady (UE)2015/2366 z dnia 25 listopada 2015 roku w sprawie usług płatniczych w ramach rynku wewnętrznego (zwana Dyrektywą PSD2), zmieniającą dyrektywy 2002/65/WE, 2009/110/WE , 2013/36/WE i rozporządzenie (UE) nr 1093/2010 oraz uchylającą dyrektywę 2007/64/WE gdzie wskazano , że aby ograniczyć ryzyko i konsekwencje m.in. nieautoryzowanych transakcji płatniczych powód powinien jak najszybciej poinformować dostawcę usług płatniczych (pozwanego) o wszelkich reklamacjach dotyczących rzekomo nieautoryzowanych transakcji płatniczych . Jak wynika z powyższego samo zaprzeczenie przez użytkownika (powoda) jakoby autoryzował transakcję płatniczą , nie jest samo w sobie potwierdzeniem braku autoryzacji.

Pozwany zarzucając powodowi rażące niedbalstwo powołał wyrok Sądu Najwyższego z dnia 10 marca 2004 roku (sygn. akt IV CK 151/03) ,w którym stwierdzono iż „ przypisanie określonej osobie niedbalstwa uznaje się za uzasadnione wtedy gdy osoba ta zachowała się w określonym miejscu i czasie w sposób odbiegający od właściwego dla niej miernika należytej staranności . Przez rażące niedbalstwo rozumie natomiast niezachowanie minimalnych (elementarnych)zasad prawidłowego zachowania się w danej sytuacji. O przypisaniu pewnej osobie winy w tej postaci decyduje więc zachowanie się przez nią w określonej sytuacji w sposób odbiegający od miernika staranności minimalnej ". Zatem powód ponosi odpowiedzialność za sporną transakcję płatniczą bowiem świadomie i wbrew postanowieniom umownym naruszył poufność narzędzi wykorzystywanych w usługach bankowości elektronicznej.

Stawiając powyższe zarzuty skarżący wniósł o :

1.zmianę zaskarżonego wyroku Sądu rejonowego w całości i orzeczenie co do istoty sprawy poprzez oddalenie powództwa w całości i zasądzenie na rzecz pozwanego kosztów procesu w tym kosztów zastępstwa procesowego według norm przepisanych oraz opłaty od pełnomocnictwa

2. zasądzenie od powoda na rzecz pozwanego zwrotu kosztów postepowania apelacyjnego w tym kosztów zastępstwa procesowego według norm przepisanych,

ewentualnie o:

1.uchylenie zaskarżonego wyroku Sądu Rejonowego w całości i przekazania sprawy do ponownego rozpoznania

2. zasądzenie od powoda na rzecz pozwanego zwrotu kosztów postepowania apelacyjnego w tym kosztów zastępstwa procesowego według norm przepisanych

W odpowiedzi na apelację powód wniósł o jej oddalenie i zasądzenie od pozwanego na swoją rzecz kosztów zastępstwa procesowego w postępowaniu apelacyjnym według norm przepisanych. W uzasadnieniu wskazał argumenty uzasadniające przyjęcie argumentów wskazanych przez pozwanego jako bezzasadne. Podnosi , iż zarzut pozwanego co do nie posiadania przez powoda wymaganych zabezpieczeń na urządzeniach , z których korzystał do obsługi bankowości elektronicznej nie jest zgodny z rzeczywistym stanem faktycznym bowiem powód zainstalował

ogólnodostępny program antywirusowy . Umowa między stronami nie zakłada zaś zainstalowania określonego programu. Podkreśla , iż ostrzeżenia Banku o zagrożeniach w cyberprzestrzeni nie mają związku ze sprawą , bowiem powód nie wiedział o jakichkolwiek przestępczych działaniach skierowanych wobec niego. Wskazuje ,że nie ma również podstaw do twierdzenia ,że sporna transakcja została autoryzowana przez powoda , bowiem sam biegły wskazał ,że transakcję należy traktować jako nieautoryzowana.

Sąd Okręgowy zważył, co następuje :

Apelacja jest bezzasadna. Zawarte w niej zarzuty i wnioski nie zasługują na uwzględnienie.

Wbrew twierdzeniom zawartym w motywach wniesionego środka odwoławczego, Sąd pierwszej instancji prawidłowo procedował w przedmiotowej sprawie i nie dopuścił żadnego z zarzucanych mu uchybień. Zarówno poczynione przez ten Sąd ustalenia, jak i dokonane oceny, Sąd Odwoławczy podziela w pełni i przyjmuje za własne (art.387& 2^1 pkt.1 i 2 k.p.c).

Apelacja nie wskazuje na żadne okoliczności, które nie byłyby przedmiotem uwagi Sądu Rejonowego i nie zawiera też takiej, merytorycznej argumentacji, która wnioskowanie tego sądu mogłaby skutecznie podważyć. Zarzuty apelacyjne w istocie swej stanowią wyłącznie polemikę z prawidłowo poczynioną przez Sąd I instancji oceną materiału dowodowego.

Odnosząc się zarzutu dotyczącego naruszenia przepisów proceduralnych tj art. 233 k.p.c. i będących ich wynikiem sprzeczności istotnych ustaleń Sądu I instancji z treścią zebranego w sprawie materiału dowodowego przede wszystkim stwierdzić trzeba, że wbrew twierdzeniom zawartym w apelacji, wszystkie istotne dla rozstrzygnięcia sprawy kwestie i dowody znalazły wyraz w toku przedmiotowego postępowania sądowego. Biorąc pod uwagę okoliczności niniejszej sprawy, zarzut wybiórczej oceny i braku wszechstronnego rozpoznania materiału dowodowego zebranego w sprawie należy uznać za całkowicie chybiony. Sąd Rejonowy w pisemnym uzasadnieniu poddał analizie cały zebrany w sprawie materiał dowodowy, a ocena tego materiału dowodowego mieści się w ramach swobodnej oceny dowodów w myśl art. 233 k.p.c. W tym miejscu przypomnieć warto, że Sąd I instancji ocenia wiarygodność i moc dowodów według własnego przekonania, na podstawie wszechstronnego rozważenia zebranego materiału, zaś to, że określony dowód został oceniony niezgodnie z intencją skarżącego, nie oznacza w żaden sposób naruszenia reguł proceduralnych, w tym zasad określonych w art. 233 k.p.c. Ocena dowodów należy bowiem do sądu orzekającego i nawet w sytuacji, w której z dowodu można było wywieść wnioski inne niż przyjęte przez Sąd nie dochodzi do naruszenia wskazanego przepisu. Analiza zgromadzonego materiału dowodowego dokonywana jest na podstawie przekonań sądu, jego wiedzy i posiadanego doświadczenia życiowego, a nadto winna uwzględniać wymagania prawa procesowego oraz reguły logicznego myślenia, według których Sąd w sposób bezstronny, racjonalny i wszechstronny rozważa materiał dowodowy jako całość, dokonuje wyboru określonych środków dowodowych i - ważąc ich moc oraz wiarygodność - odnosi je do pozostałego materiału dowodowego (patrz: wyrok Sądu Najwyższego z dnia 20 stycznia 2010 roku, II UK 154/09, Lex nr 583803).

Postawienie zarzutu obrazy przepisów prawa procesowego nie może polegać na zaprezentowaniu przez skarżącego stanu faktycznego przyjętego przez niego na podstawie własnej oceny dowodów. Skarżący może tylko wykazywać, posługując się wyłącznie argumentami jurydycznymi, że Sąd rażąco naruszył ustanowione w wymienionym przepisie zasady oceny wiarygodności i mocy dowodów oraz że naruszenie to miało wpływ na wynik sprawy.

Odnosząc się do zarzutów naruszenia przepisów prawa materialnego w ocenie Sądu Okręgowego zarzuty apelacji nie zasługiwały na uwzględnienie. W szczególności skarżący narzucił naruszenie przepisów ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych .

W związku z nowelizacją z dnia 10 maja 2018 roku ustawy o usługach płatniczych stanowiącej implementację dyrektywy unijnej PSD 2 -Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE zwaną dalej PSD 2 bank

może dokonać danej transakcji, jednak transakcja ta musi być autoryzowana przez klienta. W razie , gdy transakcja jest nieautoryzowana to wyłączną odpowiedzialność z tytułu jej przeprowadzenia ponosi dostawca usług płatniczych (pozwany bank). W sytuacji wystąpienia nieautoryzowanej transakcji pozwany jest z mocy przepisów zobowiązany do zwrotu pieniędzy objętych daną transakcją. PSD 2 wskazuje ,że bezzwłoczny zwrot oznacza zwrot w terminie nie późniejszym niż do końca następnego dnia roboczego , po odnotowaniu danej transakcji lub po otrzymaniu stosownego zgłoszenia .Dyrektywa PSD 2 wyznacza 15 dniowy termin na rozpatrzenie reklamacji , co w konsekwencji oznacza ,że klient – powód ma możliwość dysponowania kwotą nieautoryzowanej transakcji w okresie rozpatrywania reklamcji. Zatem ustawa wskazuje wręcz termin w jakim dostawca ma dokonać określonych czynności .Dopiero po wykonaniu powyższych czynności pozwany – bank ma możliwość ustalenia potencjalnej odpowiedzialności klienta – powoda. Marginalnie należałoby stwierdzić iż działania pozwanego od samego początku są zatem nieprawidłowe, bowiem bank- pozwany może odmówić zwrotu pieniędzy tylko w sytuacji kiedy ma podejrzenie co do ewentualnego popełnienia oszustwa przez klienta - powoda i poinformuje o tym niezwłocznie organy ścigania. W niniejszej sprawie nie miało to miejsca.

Odnosząc się do zarzutu pozwanego ,iż powód zawiadomił pozwanego blisko po upływie 4 miesięcy od wykonania dyspozycji przelewu nie ma znaczenia w sprawie. W tym zakresie pozwany powołał się na dyrektywę PSD 2. Zgodnie z dyrektywą PSD 2 płatnik jest zobowiązany do zgłoszenia dla dostawcy usług płatniczych nieautoryzowanej transakcji w terminie 13 miesięcy od dnia zdarzenia.

Powód udowodnił ,iż w dniu powzięcia wiadomości w wyniku spornej transakcji kwota dochodzona niniejszym pozwem nie została przelana na konto właściwe , podjął niezbędne kroki tj zawiadomił bank i organy ściągania.

Marginalnie należy zauważyć iż pozwany w zależności od sytuacji powołuje się na dyrektywę lub nie ,bowiem to pozwany zgodnie z powyższą dyrektywą miał obowiązek zwrotu dochodzonej pozwem kwoty w określonym przez dyrektywę PSD2 terminie.

Nietrafny jest zarzut pozwanego o tym ,że skoro powód był poinformowany o istniejących ryzykach i potencjalnych zagrożeniach to w związku z tym powinien był dochować należytej staranności w ochronie dostępu do swoich rachunków bankowych. Ochrona dostępu do swoich rachunków przede wszystkim powinna polegać na zamontowaniu programu antywirusowego , który to powinien zabezpieczać komputer. Biegły wskazał ,iż komputer powoda jest zabezpieczony poprzez aktualny program antywirusowy. Natomiast brak jest w regulaminie pozwanego wymogów co do rodzaju oprogramowania antywirusowego , a w szczególności czy wystarczające jest użycie ogólnodostępnych darmowych zabezpieczeń. Co więcej nie zostało udowodnione przez pozwanego w toku postępowania dowodowego przed sądem pierwszej instancji aby powód nie korzystał z wystarczających zabezpieczeń.

Powód przystępując do otwarcia dostępu do rachunku bankowego logował się na sprzęcie , wyposażonym w program antywirusowe .Logowanie odbywało się poprzez wpisanie hasła i loginu. Następnie powód przystępował do wykonania przelewów w ramach tzw koszyka przelewów .Wszyscy odbiorcy dodani do koszyka przelewów wybrani z listy odbiorów zdefiniowanych , byli zapisani w bankowości elektronicznej powoda. Jednakże sporna kwot nie trafiła do zdefiniowanego odbiorcy. Biegły jednoznacznie stwierdził ,że sporna transakcja została wykonana przez działanie szkodliwego oprogramowania typu „ malware ” , które w dniu zdarzenia funkcjonowała na komputerze powoda. Tego typu oprogramowania można nazwać typem wirusa komputerowego , który działa w tle , niezauważony przez użytkownika. Program jest ukierunkowany na bankowość elektroniczną określonych banków i działa w taki sposób ,że wyszukuje w pamięci komputera ciągi cyfr o długości 26 znaków , co odpowiada długości numeru konta bankowego w formacie (...) , który podaje się w trakcie wykonywania klasycznych przelewów bankowych . Kiedy taki ciąg zostanie wykryty ,wirus podstawia w jego miejsce swój numer konta oraz dodatkowo w odpowiednie miejsce w pamięci podstawia dane odbiorcy w postaci imienia i nazwiska. Przy czym można dodatkowo uzależnić aktywację wirusa od wskazania określonej kwoty od której się aktywuje. Pomimo bieżącej aktualizacji ochrony antywirusowej komputera ,może dojść do niewykrycia wirusa , bowiem ,żeby program antywirusowy był w stanie wykryć danego wirusa , twórca oprogramowania wirusowego musiałby najpierw wprowadzić tzw sygnaturę wirusa do bazy programu antywirusowego (coś na kształt wzoru programu) , który ma zostać finalnie wykryty przez system antywirusowy. W

obecnych czasach twórcy programów antywirusowych nie nadążają z uwzględnieniem tego typu wirusów w swoich produktach .

Zatem doszło w niniejszej sprawie do przełamania zabezpieczenia komputera powoda .Nie doszło do przełamania zabezpieczeń bankowych .Na szczególną uwagę zasługuje fakt ,iż przy tzw koszyku przelewów po wprowadzeniu wszystkich przelewów do zdefiniowanych odbiorców powód otrzymuje sms kod który to po wprowadzeniu powoduje swoistego rodzaju autoryzację koszyka przelewów. W niniejszej sprawie system pozwanego wysłał dodatkowego sms z kodem dla powoda z uwagi na pojawienie się rachunku E. M. zamiast (...) sp.z o.o. bowiem była to pierwsza transakcja na ten numer rachunku. Jednakże jak słusznie zauważył biegły powód otrzymał od pozwanego wiadomość sms z informacją o dodaniu nowego przelewu bez informacji ani o odbiorcy ani o kwocie, a wysłanie tej informacji miało miejsce jedynie dlatego ,że numer rachunku E. M. pojawił się po raz pierwszy w historii rachunku powoda. Powód zatem nie był wcześniej informowany przez pozwanego ,że w takiej sytuacji powinien wstrzymać się z dokonaniem przelewu zwłaszcza ,że praktyka banków w zakresie potwierdzania transakcji kodem SMS jest powszechna. Zatem z punktu widzenia systemu bankowego sporna transakcja może być uznana za autoryzowaną bowiem została ona potwierdzona kodem przesłanym przez pozwanego w wiadomościach sms. Jednakże skoro autoryzacja tej transakcji została uzyskana poprzez doprowadzenie użytkownika bankowości elektronicznej (powoda) postępem do autoryzacji transakcji, której de facto nie chciał wykonać poprzez podmianę danych faktycznych odbiorcy to taka transakcja jest traktowana jako nieautoryzowana.

Przechodząc do zarzuty pozwanego co do rażącego niedbalstwa powoda należy podkreślić ,iż Sąd nie znalazł w działaniu powoda cech , którym można przepisać rażące niedbalstwo.

Zgodnie z treścią art. 355 § 1 k.c. dłużnik obowiązany jest do staranności ogólnie wymaganej w stosunkach danego rodzaju. Przy czym rażące niedbalstwo jest kwalifikowaną formą winy nieumyślnej i sprowadza się do wyraźnego braku staranności działania Chodzi głównie o takie zachowanie , które graniczy z umyślnością (wyrok SN z dnia 29 stycznia 2009 r V CSK 291/08).Sąd pierwszej instancji słusznie wskazał na brak rażącego niedbalstwa w działaniach powoda , bowiem gdyby w momencie wykonywania spornej transakcji powód miał jasną informację ,że transakcja ma być wykonana na inny rachunek odbiorcy niż (...) sp. z o.o. to kodu autoryzacyjnego z wiadomości SMS przesłanej przez pozwanego by nie wprowadził , a tym samym do autoryzacji transakcji w systemie bankowości elektronicznej by nie doszło.

Skarżący zarzucił ponadto naruszenie przepisów tj art. 40 i 46 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych, która to reguluje rynek usług płatniczych w zakresie zasad prowadzenia działalności na rynku usług płatniczych jak i prawa i obowiązki dostawców usług płatniczych związane ze świadczeniem usług płatniczych .W ustawie tej uregulowano kwestie związane z autoryzacją transakcji płatniczych, skutków braku autoryzacji transakcji oraz zasad odpowiedzialności dostawcy i płatnika za transakcje nieautoryzowane.

Przepisy ustawy nakładają na dostawcę udowodnienie ,że transakcja płatnicza została autoryzowana przez płatnika , przy czym samo wykazanie faktu ,że doszło do autoryzacji (wpisanie kodu z SMS) jeszcze nie oznacza ,że transakcja została autoryzowana przez płatnika. W okolicznościach wskazywanych przez pozwanego odpowiedzialność banku byłaby praktycznie na zawsze wyłączona , bowiem wpisanie kodu z SMS oznaczałoby automatyczne uznanie ,że mamy do czynienia z transakcją autoryzowaną. Jednakże powód udowodnił iż transakcja była nieautoryzowana poprzez złożenie wniosku o biegłego , który to jednoznacznie potwierdził iż w przedmiotowej sprawie nie doszło do autoryzacji z uwagi na brak winy powoda.

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. 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. 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,to 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 albo wskutek rażącego niedbalstwa naruszył jeden z obowiązków określonych w art. 42 ustawy o transakcjach płatniczych czyli nie przechowywał informacji w sposób zapewniający bezpieczeństwo.

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.

Należy wskazać iż ,zgodnie natomiast z art. 40 ust. 1 ustawy o usługach płatniczych transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zgoda może dotyczyć także kolejnych transakcji płatniczych. A contrario, z nieautoryzowaną transakcją płatniczą mamy do czynienia w sytuacji, gdy płatnik nie wyraził na nią zgody.

Z przeprowadzonego postepowania dowodowego przed sądem pierwszej instancji wynika jednoznacznie ,że transakcji powoda nie można uznać za autoryzowaną w rozumieniu powyżej cytowanego przepisu. Powód nie wyraził zgody na tę transakcję , o czy świadczy jego natychmiastowa reakcji , po stwierdzeniu ,że pieniądze zostały przelane na konto osoby trzeciej tj zawiadomienie banku oraz policji o popełnieniu przestępstwa. Tym samym powód wypełnił obowiązek wynikający za art.44 ustawy o usługach płatniczych . Z tych też względów , zdaniem Sądu nieuzasadnione byłoby przyjęcie , zwalniające pozwany bank z odpowiedzialności .

W konsekwencji, na gruncie art. 46 ust. 1 tej ustawy o usługach płatniczych należy przyjąć, że w przedmiotowym przypadku wystąpiła nieautoryzowana transakcja płatnicza uprawniająca płatnika do żądania od jego dostawcy zwrotu kwoty nieautoryzowanej transakcji płatniczej. Dlatego słusznie Sąd Rejonowy doszedł do wniosku, że roszczenie powoda miało oparcie w tym przepisie. Sąd Okręgowy uznał odpowiedzialność pozwanego Banku wobec powoda także na podstawie art. 471 k.c. w związku z art. 725 k.c.

Mając zatem powyższe na uwadze, nie podzielając zarzutów ani wniosków zawartych w apelacji, Sąd Okręgowy na podstawie art. 385 k.p.c. oddalił apelację. O kosztach procesu orzeczono na podstawie art. 98 k.p.c, zgodnie z zasadą, iż strona przegrywająca sprawę obowiązana jest zwrócić przeciwnikowi na jego żądanie koszty niezbędne do celowego dochodzenia praw i celowej obrony.

Sędzia Iwona Nowak

.

\