Sygn. akt IX Ca 109/24 upr.

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 25 marca 2024 r.

Sąd Okręgowy w Olsztynie IX Wydział Cywilny Odwoławczy

w składzie:

Przewodniczący:	SSO Jacek Barczewski
Protokolant:	st. sekr. sąd. Marta Borowska

po rozpoznaniu w dniu 20 marca 2024 r. w Olsztynie

na rozprawie

sprawy z powództwa W. S.

przeciwko Bankowi (...) Spółce Akcyjnej z siedzibą w W.

o zapłatę

na skutek apelacji pozwanego od wyroku Sądu Rejonowego w Mrągowie z dnia 29 listopada 2023 r., sygn. akt I C 600/21,

I. zmienia zaskarżony wyrok w punkcie I w ten tylko sposób, że odsetki ustawowe za opóźnienie od wskazanej tam kwoty 6.000 (sześć tysięcy) zł zasądza od dnia 8 lutego 2020 r. do dnia zapłaty, oddalając powództwo w pozostałym zakresie,

II. oddala apelację w pozostałej części,

III. zasądza od pozwanego na rzecz powódki kwotę 900 (dziewięćset) zł tytułem zwrotu kosztów procesu za instancję odwoławczą z odsetkami ustawowymi za opóźnienie za czas od dnia uprawomocnienia się niniejszego orzeczenia o kosztach do dnia zapłaty.

Jacek Barczewski

Sygn. akt: IX Ca 109/24 upr.

UZASADNIENIE

Powódka W. S. wniosła o zasądzenie od pozwanego Banku (...) S.A. z siedzibą w W. na jej rzecz kwoty 6.000 złotych z odsetkami ustawowymi za opóźnienie od dnia 7 lutego 2020 roku do dnia zapłaty tytułem zwrotu należności wynikającej z nieautoryzowanych transakcji płatniczych.

W uzasadnieniu wskazała, że posiada rachunek bankowy u pozwanego. Dnia 5 lutego 2020 roku kliknęła w reklamę pozwanego Banku. Została przekierowana na stronę łudząco podobną do strony banku, gdzie wymagano podania kodu oraz numeru pesel. Wskazała, że nie wpisywała żadnych danych na stronie banku oraz nie dokonywała na

nim żadnych transakcji. Kolejnego dnia zauważyła na swoim telefonie wiadomość napisaną w języku angielskim. Następnie z powódką skontaktował się pracownik pozwanego banku i poinformował ją, że z jej rachunku została wybrana kwota 920 złotych. Powódka tego samego dnia udała się do placówki banku. Okazała się, że na jej rachunku dokonano trzech transakcji, co spowodowało wyprowadzenie z jej rachunku kwoty 1234,19 euro. Powódka złożyła reklamację w placówce banku. Złożyła również zawiadomienie o popełnieniu przestępstwa.

Nakazem zapłaty w postępowaniu upominawczym z dnia 23 listopada 2021 roku w sprawie I Nc 332/21 referendarz sądowy Sądu Rejonowego w Mrągowie nakazał pozwanemu Bankowi (...) S.A. z siedzibą w M., aby zapłacił powódce W. S. kwotę 6000 złotych wraz z odsetkami ustawowymi za opóźnienie od dnia 7 lutego 2020 roku do dnia zapłaty oraz kwotę 1817 złotych tytułem kosztów postępowania wraz z odsetkami ustawowymi za opóźnienie za czas od dnia uprawomocnienia się orzeczenia do dnia zapłaty, w tym kwotę 1200 złotych tytułem kosztów zastępstwa procesowego, w terminie dwóch tygodni od doręczenia nakazu albo wniósł w tym terminie sprzeciw.

Pozwany złożył sprzeciw od nakazu zapłaty. Wniósł o oddalenie powództwa w całości.

W uzasadnieniu wskazał, że powódka nie przedstawiła żadnych dowodów na to, że autoryzacja transakcji została rzeczywiście dokonana przez osobę trzecią bez wiedzy i woli powódki. Gdyby rzeczywiście autoryzacja została dokonana przez osobę trzecią to i tak wyłączną przyczyną utraty środków przez powoda z rachunku bankowego jest brak dbałości powoda o swoje interesy. Bank podjął wszelkie działania mające uniemożliwić dokonywanie nieautoryzowanych transakcji na kontach swoich klientów, w tym na koncie powoda. Bank wprowadził szereg wymogów, które gwarantują, że osobą która rzeczywiście dokonuje transakcji, jest podmiot umowy z Bankiem. Po weryfikacji zgłoszenia powódki Bank ustalił, że logowanie do systemu Millnet przebiegło prawidłowo. W dniach 5-6 lutego 2020 roku po prawidłowym zalogowaniu się do bankowości internetowej aktywowana została aplikacja mobilna Banku, następnie zmieniono limit dla rachunku oraz został dodany zaufany odbiorca przez potwierdzenie hasłem sms wysłanym na numer telefonu powoda. Jak wskazuje sama powódka, sporne transakcje mogą być powiązane z jej działaniem w Internecie, gdzie umieszczona została reklama podmiotu prawdopodobnie podszywającego się pod pozwany Bank. W ocenie pozwanego, oparcie zaufania do strony internetowej tylko i wyłącznie na jej szacie graficznej, bez sprawdzenia szyfrowania połączeń odpowiednim protokołem SSL, świadczy o niedochowaniu należytej staranności po stronie powoda i jako takie może obciążać tylko jego.

Wyrokiem z dnia 29 listopada 2023 r. Sąd Rejonowy w Mrągowie w punkcie I. zasądził od pozwanego na rzecz powódki kwotę 6.000 zł z odsetkami ustawowymi za opóźnienie od dnia 7 lutego 2020 r. do dnia zapłaty i w punkcie II. zasądził od pozwanego na rzecz powódki kwotę 2.463,73 zł wraz z odsetkami ustawowymi za opóźnienie od dnia uprawomocnienia się orzeczenia do dnia zapłaty tytułem zwrotu kosztów procesu, w tym kwotę 1.800 zł tytułem kosztów zastępstwa procesowego.

Sąd Rejonowy ustalił następujący stan faktyczny: Powódka W. S. zawarła z pozwanym Bankiem (...) S. A. z siedzibą w W. umowę bieżącego rachunku bankowego. Korzystała również z usług bankowości internetowej. W dniu 5 lutego 2020 roku powódka korzystając z Internetu na domowym komputerze zauważyła reklamę łudząco podobną do reklamy pozwanego Banku. Z reklamy tej wynikało, że Bank przygotował dodatkowe korzyści dla swoich klientów. Powódka kliknęła w tę reklamę. W ten sposób otworzyła stronę łudząco podobną do strony Banku. Następnie wykonała czynności logowania się na swoje konto w pozwanym Banku. W tym czasie osoby trzecie wykorzystując dane uzyskane od powódki zalogowały się w kanale bankowości internetowej pozwanego Banku a następnie aktywowały aplikację mobilną Banku. Zmieniły limit na rachunku oraz dodały zaufanego odbiorcę przez potwierdzenie hasłem sms wysłanym na numer telefonu powódki. Następnie zlecony został przelew z Konta 360 stopni powódki na kwotę 920 złotych oraz przelewy z konta walutowego na kwoty 728,85 euro, 211,37 euro, 293,97 euro na konto zaufanego odbiorcy, (przez co nie wymagały potwierdzenia hasłem sms). Dodatkowo zostały zrealizowane przelewy wewnętrzne z Konta Oszczędnościowego EUR na konto bieżące EUR na kwoty 300 euro i 50 euro. Transakcje w dniu 6 lutego 2020 roku były dokonywane z urządzeń wykorzystujących adresy IP lokalizowane jako te, które są przypisane do sieci w Rosji. W tym czasie powódka otrzymała dwie wiadomości sms w języku polskim i jedną w języku angielskim. W dniu 6 lutego 2020 r. około godziny 10.30 z powódką skontaktował się telefonicznie pracownik pozwanego Banku. Wskazał,

że z konta powódki została pobrana kwota 920 złotych. Poinformował powódkę, że skoro nie zlecała wykonania takiej transakcji to powinna dokonać zgłoszenia reklamacyjnego. Tego samego dnia powódka udała się do placówki Banku. Dowiedziała się, że na jej rachunku walutowym dokonane zostały trzy transakcje, co spowodowało pobranie z tego rachunku kwoty łącznej 1234,19 euro. W trakcie tej wizyty w palcówce Banku powódka zgłosiła reklamację, co do wykonania tych transakcji. Tego samego dnia W. S. zgłosiła na Policję zawiadomienie o popełnieniu przestępstwa na jej szkodę.

Kolejno tenże Sąd ustalił, że pismem z dnia 26 lutego 2020 r. pozwany Bank poinformował powódkę, że nie ma podstaw do uznania reklamacji i zwrotu kwoty przelewów z 5-6 lutego 2020 roku. Postanowieniem z dnia 30 czerwca 2020 r., zatwierdzonym przez Prokuratora Prokuratury Rejonowej w Mrągowie, umorzono postępowanie o czyn z art. 287 § 1 k.k. z powodu niewykrycia sprawy przestępstwa. W toku postępowania dopuszczono dowód z opinii biegłego z zakresu informatyki i bezpieczeństwa systemów informatycznych w celu wykazania związku działania powódki w zakresie udostępnienia danych karty płatniczej w Internecie osobom trzecim z możliwością wykonania spornych transakcji na rachunku powódki, przebiegu transakcji w systemie transakcyjnym banku, zakresu wymaganych do podjęcia przez powódkę czynności mogących uniemożliwić zaistnienie przedmiotowego zdarzenia. Biegły M. M. we wnioskach opinii z dnia 16 marca 2023 roku wskazał, że badania potwierdziły schemat działania powódki i pozwanego oraz w ocenie biegłego potwierdziły przypadek ataku phishingowego. Zapis logów potwierdził przedstawioną w aktach sekwencję wydarzeń oraz potwierdził, że pozwany dokonał wszelkich czynności znanych na tamten czas uznanych jako bezpieczne podczas dokonywania transakcji w systemie bankowości elektronicznej. Wątpliwości może budzić fakt, iż na podstawie danych archiwalnych możliwe było ujawnienie anomalii w schemacie zachowań użytkownika (inny adres IP), jednak należy to traktować bardziej jako niedoskonałość niż wadę systemu lub jego przełamanie. Zmiana adresu IP nie jest jednoznaczną przesłanką, która jednostkowo mogłaby obligować system do podjęcia działań anty kradzieżowych. W istocie systemy klasy IDS oraz IPS powinny analizować wszelkie anomalia historyczne czy sekwencje wydarzeń typowe dla prób działań przestępczych w celu ich uniknięcia. W opinii biegłego, działanie systemu było poprawne, a pozwany posiadał poprawne zabezpieczenia. Powódka poprzez umieszczenie danych identyfikacyjnych przekazała dane atakującym, którzy następnie mogli użyć tych danych w kontynuacji ataku. W opinii uzupełniającej biegły wskazał, że poza jego kognicją są rozważania polegające na ocenie działań jakiejkolwiek ze stron pod kątem prawnym. W istocie analizując sekwencje wydarzeń pod kątem technologicznym należy stwierdzić, że z dużym prawdopodobieństwem powódka została zaatakowana atakiem socjotechnicznym wykorzystującym elementy technologiczne do wykonania transakcji na jej koncie bankowym. W związku z powyższym, w ocenie biegłego, można wykluczyć umyślność w działaniu powódki. Jak zauważył Sąd Rejonowy pojęcie rażącego niedbalstwa jest w przypadku analizowanej sprawy pojęciem prawniczym w związku z powyższym biegły nie może zająć stanowiska. Faktem jest, że powódka została zmanipulowana i oszukana przez osoby trzecie, a możliwością zapobiegania takim incydentom jest uważna weryfikacja wykonywanych czynności w sieci Internet.

W tak ustalonym stanie faktycznym Sąd Rejonowy doszedł do wniosku, że powództwo jest zasadne. Stosownie do art. 725 k.c. 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 rachunku bankowością internetową. Jak zauważył tenże Sąd, równoległą podstawą odpowiedzialności banku jest ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (jedn. tekst: Dz.U. z 2017 r., poz. 2003 ze zm.; dalej: „u.o.u.p."). Sąd I instancji przyjął, że zgodnie z art. 45 i 46 u.o.u.p., transakcje dokonane na rachunku powódki w dniach 5-6 lutego 2020 roku nie były autoryzowane, gdyż zostały wykonane przez osobę nieuprawnioną. Z tych przepisów w sposób jednoznaczny wynika obowiązek udowodnienia przez pozwanego, iż powódka umyślnie doprowadziła do rzeczonej transakcji płatniczej albo umyślnie lub przez rażące niedbalstwo naruszyła obowiązki wynikające z art. 42 ustawy. Natomiast w realiach niniejszej sprawy pozwany nie przedstawił żadnych dowodów w tym zakresie, ale poprzestał jedynie na przypuszczeniach co do sposobu dokonania spornej transakcji. Sąd Rejonowy wskazał, że o umyślnym doprowadzeniu do nieautoryzowanej transakcji płatniczej nie może świadczyć sam fakt podjęcia przez powódkę w dniu 5 lutego 2020 roku nieudanej próby logowania. Powódka dokonała tej czynności po kliknięciu w reklamę Banku i na stronie łudząco podobnej graficznie do strony internetowej Banku. Strona ta była na tyle podobna do strony Banku, iż nie budziła wątpliwości powódki.

Kolejno Sąd I instancji wskazał, że zgodnie z art. 42 ust. 1 pkt 1 i 2 oraz ust. 2 u.o.u.p., użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany korzystać z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. W celu spełnienia obowiązku, o którym mowa w ust. 1 pkt 1, użytkownik, z chwilą otrzymania instrumentu płatniczego, podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych zabezpieczeń tego instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym. Zdaniem tego Sądu w niniejszej sprawie nie ma podstaw do przyjęcia, że powódka naruszyła obowiązek korzystania z instrumentu płatniczego zgodnie z umową ramową lub obowiązek zgłoszenia dostawcy (Bankowi) utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. Do utraty pieniędzy z rachunku bankowego powódki nie doszło bowiem w okolicznościach opisanych w przytoczonych przepisach, ale wskutek popełnienia przestępstwa przez nieustaloną osobę trzecią, która skorzystała z niewłaściwego zabezpieczenia przez Bank świadczenia usługi bankowości internetowej. Z opinii biegłego z zakresu informatyki i bezpieczeństwa systemów informatycznych M. M. wynikało, że wprawdzie pozwany Bank dokonał wszelkich czynności znanych na tamten czas uznanych jako bezpieczne podczas dokonywania transakcji w systemie bankowości elektronicznej jednak system ten był niedoskonały, gdyż nie sygnalizował anomalii w schemacie zachowań użytkownika (inny adres IP), system nie podjął działań antykradzieżowych. Biegły wskazał, że w istocie systemy klasy IDS oraz IPS powinny analizować wszelkie anomalia historyczne czy sekwencje wydarzeń typowe dla prób działań przestępczych w celu ich uniknięcia.

Jak zauważył Sąd Rejonowy w opinii uzupełniającej biegły dodatkowo wskazał, że z dużym prawdopodobieństwem powódka została zaatakowana atakiem socjotechnicznym wykorzystującym elementy technologiczne do wykonania transakcji na jej koncie bankowym. W związku z powyższym, w ocenie biegłego, można wykluczyć umyślność w działaniu powódki. Ponadto powódka została zmanipulowana i oszukana przez osoby trzecie. W związku z powyższym w ocenie Sądu działaniom powódki nie można przypisać zarówno umyślności, jak i rażącego niedbalstwa, o których mowa w art. 42 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych. Z uwagi na powyższe Sąd I instancji uznał, że powództwo zasługuje na uwzględnienie w całości i zasądził od pozwanego Banku (...) S.A. z siedzibą w W. na rzecz powódki W. S. kwotę 6000 złotych z odsetkami ustawowymi za opóźnienie od dnia 7 lutego 2020 roku do dnia zapłaty. O kosztach procesu tenże Sąd orzekł w punkcie II. wyroku - stosownie do jego wyniku - na podstawie art. 98 § 1, § 1^1 i § 3 k.p.c. i art. 99 k.p.c. w zw. z § 2 pkt 2 i § 15 ust. 1 Rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 roku w sprawie opłat za czynności radców prawnych (tekst jednolity: Dz. U. z 2018r. poz. 265), zasądzając od pozwanego na rzecz powódki kwotę 2.463,73 złotych tytułem zwrotu kosztów procesu, w tym kwotę 1.800 złotych tytułem kosztów zastępstwa procesowego.

Od wyroku Sądu I instancji apelację wniósł pozwany, zaskarżając wyrok w całości i zarzucając:

1. naruszenie przepisów postępowania mające istotny wpływ na treść zaskarżonego rozstrzygnięcia, tj.:

a) naruszenie z art. 233 § 1 k.p.c. w zw. z art. 299 k.p.c., poprzez oparcie ustaleń faktycznych na zeznaniach powódki W. S. w zakresie, w jakim były one niewiarygodne i sprzeczne z zasadami logiki i doświadczenia życiowego oraz były sprzeczne z dokumentami zgromadzonymi w sprawie, co miało wpływ na rozstrzygnięcie, ponieważ doprowadziło Sąd I instancji do nieprawidłowych ustaleń faktycznych opisanych poniżej, które doprowadziły Sąd I instancji do przekonania o nieautoryzowaniu spornych transakcji przez powódkę, a w konsekwencji Sąd I instancji uwzględnił roszczenie powódki o zapłatę;

b) naruszenie art. 243^2 k.p.c. w zw. z art. 235^2 § 1 i § 2 k.p.c. w zw. z art. 227 k.p.c. w zw. z art. 327^1 § 1 ust. 1 k.p.c. poprzez brak szczegółowego odniesienia się w uzasadnieniu do dowodów załączonych do sprzeciwu od nakazu zapłaty, tj. dowodu z następujących dokumentów:

- Regulaminu ogólnego świadczenia usług bankowych dla osób fizycznych w Banku (...) S.A.,

- Wydruku ze strony internetowej Banku dot. bezpieczeństwa przy korzystaniu z bankowości internetowej,

które to dowody miały istotne znaczenie dla rozstrzygnięcia sprawy, ponieważ dowodziły m.in. faktu spełnienia przez Bank wszystkich wymagań w zakresie zabezpieczenia systemu transakcyjnego Banku przy procesowaniu przedmiotowej transakcji, związku zainfekowania urządzenia powódki złośliwym oprogramowaniem z możliwością wykonania spornych transakcji na rachunku powódki, przebiegu transakcji w systemie transakcyjnym Banku, wyłącznej winy powódki w doprowadzeniu do przejęcia kontroli nad telefonem powódki, braku odpowiedzialności Banku za niestaranne zachowanie powódki, informowania powódki o zasadach bezpiecznego korzystania z systemów transakcyjnych Banku, w tym konieczności instalowania oprogramowania antywirusowego oraz nieinstalowania aplikacji niepochodzących od zaufanych dostawców, spełnienia przez Bank wszystkich wymagań w zakresie zabezpieczenia systemu transakcyjnego Banku przy procesowaniu przedmiotowej transakcji, wyłącznej winy powódki w doprowadzeniu do przejęcia kontroli nad telefonem powódki, braku odpowiedzialności Banku za niestaranne zachowanie powódki, co w konsekwencji doprowadziło do błędnego przyjęcia przez Sąd I instancji, że sporne transakcje nie zostały autoryzowane przez powódkę, a naruszenie to miało wpływ na rozstrzygnięcie, ponieważ oparcie się na ww. dowodach przekładałoby się na ocenę, że Bank nie ponosi odpowiedzialności za dokonanie spornych transakcji;

c) art. 233 § 1 k.p.c. przez dokonanie sprzecznej z zasadami logiki i doświadczenia życiowego, dowolnej, a nie swobodnej oceny dowodów, pozbawionej wszechstronnego i obiektywnego rozważenia całości materiału dowodowego i wyciągnięcie na tej wadliwej podstawie bezpodstawnych i niezgodnych z rzeczywistym stanem faktycznym wniosków leżących u podstaw wyroku, w szczególności przez bezpodstawne przyjęcie, że:

i. powódka nie wiedziała o błędnym logowaniu do bankowości elektronicznej, nie musiała wiedzieć o różnicy w sposobie logowania do aplikacji bankowej, podczas gdy - jak zeznała sama powódka - od wielu lat używała strony Banku, konto w Banku posiadała 17 lat, a zatem miała świadomość w zakresie standardowego procesu logowania i autoryzacji transakcji, co więcej - logowanie do rzekomej bankowości elektronicznej banku nie odbyło się na stronie internetowej należącej do Banku (...) S.A. a poprzez reklamę na portalu Facebook;

ii. powódka padła ofiarą phishingu, a jej dane logowania do bankowości elektronicznej zostały wykradzione bez jej wiedzy, podczas gdy - jak wynika z zeznań powódki - powódka mogła uniknąć wyjawienia danych autoryzacyjnych poprzez chociażby sprawdzenie adresu wyświetlonej strony, czego powódka nie zrobiła;

2. naruszeniu przepisów prawa materialnego, a to:

a) art. 46 ust. 1 ustawy o usługach płatniczych poprzez uznanie, że sporne transakcje płatnicze stanowią „nieautoryzowane transakcje płatnicze", o których mowa w tym przepisie, co skutkowało uznaniem, że Bank jest zobowiązany do zwrotu spornych kwot podczas gdy z materiału dowodowego nie wynika kto konkretnie posługiwał się danymi powódki, a sprawstwo osoby trzeciej nie zostało do tej pory prawomocnie potwierdzone;

b) art. 45 ust 2 zdanie 2 u.o.u.p., poprzez błędne uznanie, że pozwany nie udowodnił, że sporne transakcje były autoryzowane, podczas gdy z umowy łączącej strony oraz z treści § 46 ust. 2 Regulaminu Ogólnego Świadczenia Usług Bankowych dla Osób Fizycznych w Banku (...) wynika, że transakcje uważa się za autoryzowane jeżeli zostaną potwierdzone poprzez użycie jednorazowych haseł sms Banku na zdefiniowany w Millenet (system komunikacji internetowej) numer telefonu komórkowego;

c) art. 42 ust. 1 pkt 1 oraz ust. 2 u.o.u.p. poprzez błędne uznanie, że powódka podjęła niezbędne środki zapobiegające naruszeniu indywidualnych zabezpieczeń instrumentu, w szczególności obowiązku przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym, w sytuacji gdy powódka nie sprawdziła adresu strony internetowej, na którą nastąpiło logowanie, kliknęła w reklamę rzekomo należącą do Banku na portalu Facebook;

d) art. 46 ust. 3 u.o.u.p. poprzez błędne niezastosowanie tego przepisu w sytuacji, w której powódka odpowiada za nieautoryzowane transakcje w pełnej wysokości gdyż doprowadziła do nich wskutek rażącego niedbalstwa polegającego na zalogowaniu się do konta Bankowego na stronie, bez sprawdzenia jej adresu i „niepatrzenia na adres strony internetowej", co wynika z zeznań powódki.

Pozwany wniósł o zmianę zaskarżonego wyroku w całości i oddalenie powództwa wobec Banku w całości, ewentualnie o uchylenie wyroku w całości i przekazanie sprawy do ponownego rozpoznania Sądowi I instancji, a w każdym alternatywnym przypadku o zasądzenie od powódki na rzecz pozwanego kosztów procesu za postępowanie w I instancji oraz za postępowanie w II instancji, w tym kosztów zastępstwa procesowego oraz opłaty skarbowej od pełnomocnictwa, według norm przepisanych.

W odpowiedzi na apelację powódka wniosła o oddalenie apelacji w całości i o zasądzenie od pozwanego na rzecz powódki zwrotu kosztów procesu, w tym kosztów zastępstwa procesowego za instancję odwoławczą, według norm przepisanych.

Sąd Okręgowy zważył, co następuje:

Apelacja strony pozwanej okazała się w przeważającej mierze bezzasadna. Jedynie w zakresie rozstrzygnięcia w przedmiocie zasądzonych od należności głównej ustawowych odsetek za opóźnienie Sąd Okręgowy doszedł do wniosku, że odsetki te należą się nie jak zasądził Sąd I instancji, tj. od dnia 7 lutego 2020 r., tylko od dnia 8 lutego 2020 r. do dnia zapłaty. W pozostałym zakresie apelacja i podniesione w niej zarzuty są niezasadne.

Sąd Okręgowy zasadniczo podziela i przyjmuje za własne ustalenia faktyczne Sądu I instancji jak również przedstawioną w uzasadnieniu wyroku tego Sądu ocenę prawną, choć z pewnymi uwagami wynikającymi z dalszej części uzasadnienia.

Zgodnie z art. 46 ust. 3 ustawy o usługach płatniczych 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. Zgodnie zaś z art. 42 ust. 1 ustawy użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany: 1) korzystać z instrumentu płatniczego zgodnie z umową ramową oraz 2) zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. Natomiast zgodnie z ustępem 2 omawianego przepisu w celu spełnienia obowiązku, o którym mowa w ust. 1 pkt 1, użytkownik, z chwilą otrzymania instrumentu płatniczego, podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym.

W ocenie Sądu Okręgowego nie ulega wątpliwości, że w niniejszej sprawie doszło do nieautoryzowanych transakcji płatniczych, natomiast oś sporu sprowadza się do oceny, czy płatnik, tj. powódka ponosi za nie odpowiedzialność, innymi słowy czy powódka doprowadziła do tych transakcji umyślnie, albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków wskazanych w art. 42 ust. 1-2 ustawy. W ocenie Sądu Okręgowego nie budzi wątpliwości, że powódka nie doprowadziła do spornych transakcji umyślnie, ponieważ to nie ona owe transakcje zainicjowała. Transakcje zostały przeprowadzone bez udziału powódki tj. bez jej wiedzy i woli przez osoby trzecie, które uzyskały dostęp do konta powódki w bankowości elektronicznej na skutek wprowadzenia powódki w błąd. Jak wynika ze zgromadzonego w sprawie materiału dowodowego powódka kliknęła na reklamę, która przekierowała powódkę na stronę łudząco podobną do strony pozwanego banku. Powódka wpisała na tej stronie dane do logowania do bankowości internetowej, tj. Mille kod oraz numer Pesel. W ten sposób osoby trzecie uzyskały dostęp do konta powódki w bankowości internetowej. (vide protokół zawiadomienia o możliwości popełnienia przestępstwa, załączone akta PR.DS.156.2020, k. 6)

Nie budzi zatem wątpliwości, że powódka naruszyła co najmniej jeden z obowiązków wskazanych w art. 42 ust. 1-2 ustawy przy czym naruszenie to nie miało charakteru umyślnego, bowiem, co raz jeszcze należy zauważyć, powódka udostępniła osobom trzecim dane umożliwiające zalogowanie do jej konta w bankowości internetowej w sposób nieświadomy.

Jak wynika z informacji nadesłanej do powódki z pozwanego banku (pismo k. 17) Bank zaewidencjonował czynności zlecone po prawidłowym zalogowaniu w Millenet potwierdzone hasłem sms wysłanym na wskazany przez powódkę numer telefonu: w dniu 5 lutego 2020 r. operacja nr 1 dodanie nowego odbiorcy zaufanego oraz operacja nr 2 nowy limit gotówkowy 15.000 zł i w dniu 6 lutego 2020 r. został wysłany sms zawierający kod do aktywowania aplikacji mobilnej ze wskazówką by nikomu go nie przekazywać (treść smsa w języku angielskim którego, jak wynika z przesłuchania powódki, powódka nie zrozumiała). Następnie zostały zlecone przelewy z konta powódki, które nie wymagały już potwierdzenia hasłem przesłanym we wiadomości sms, ponieważ zostały zlecone do zaufanego odbiorcy. Tymczasem z pisma skierowanego przez pozwany Bank do Biura Rzecznika Finansowego wynika, że w przypadku powódki Bank zaewidencjonował następujące transakcje mające miejsce w dniu 6 lutego 2020 r. na rachunku powódki po zalogowaniu w kanale bankowości elektronicznej - Millenet potwierdzone hasłem sms wysłanym na wskazany przez klientkę numer telefonu. Aktywowano aplikację mobilną. Zwiększono limit główny transakcji do 15.000 PLN. Dodano nowego odbiorcę zaufanego, a następnie wykonano przelewy do odbiorcy zaufanego, które nie wymagały potwierdzenia hasłem sms (pismo k. 25). Przedstawiona w obydwu pismach sekwencja zdarzeń nie jest zatem tożsama, a pozostały, zgromadzony w sprawie materiał dowodowy nie pozwala jednoznacznie rozstrzygnąć, który opis zdarzeń zgodny jest ze stanem faktycznym.

Jednocześnie powódka zaprzeczyła aby cokolwiek autoryzowała, potwierdziła jedynie, że zalogowała się na stronie łudząco podobnej do strony Banku, podając Pesel i kod (przesłuchanie powódki protokół z dnia 7 czerwca 2022 r., k. 82-83). Jak wynika z opinii biegłego M. M., pozwany zabezpieczył transakcje na kilka sposobów: poprzez autoryzację użytkownika, poprzez przesłanie kodu sms, zatem innym kanałem komunikacji o treści wskazującej na wykonywany przelew, poprzez weryfikację poprawności kodu SMS (opinia k. 144 v.).

Podsumowując tę część rozważań, w niniejszej sprawie poza sporem jest, że powódka podała na stronie internetowej łudząco podobnej do strony pozwanego Banku dane logowania, tj. Millekod oraz Pesel. Powódka naruszyła zatem obowiązek zachowania poufności danych służących do logowania do konta w bankowości internetowej (art. 42 ust. 1 – 2 ustawy o usługach płatniczych). Jak wynika z opinii biegłego samo zalogowanie do bankowości internetowej nie daje jednak możliwości dokonywania transakcji w dowolny sposób, wymagają one bowiem potwierdzenia poprzez kod SMS. W przypadku powódki został dodany odbiorca zaufany, a zatem sama transakcja przelewu nie wymagała podania kodu. Niemniej jednak, podania takiego kodu wymagało zwiększenie limitu transakcji oraz dodanie zaufanego odbiorcy (pismo pozwanego k. 17). Ze zgromadzonego w sprawie materiału dowodowego nie wynika jednak w jaki sposób (i czy w ogóle) powódka udostępniła osobom trzecim kody, które autoryzowałyby czynności zwiększenia limitu transakcji oraz dodania zaufanego odbiorcy. W związku z powyższym, zdaniem Sądu Okręgowego pozwany nie udowodnił, że powódka udostępniła osobom trzecim dane niezbędne do przeprowadzenia spornych transakcji.

Tymczasem zgodnie z art. 45 ust. 1 ustawy o usługach płatniczych ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Według art. 45 ust. 2 ustawy, 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 (vide wyrok Sądu Najwyższego z dnia 18 stycznia 2018 r. w sprawie V CSK 141/17). W orzecznictwie przyjmuje się, że samo podanie danych umożliwiających zalogowanie do bankowości elektronicznej, w sytuacji gdy dla autoryzacji (potwierdzenia) czynności potrzebne jest jeszcze podanie kodów autoryzacyjnych przesłanych w treści wiadomości sms, nie stanowi jeszcze przejawu rażącego niedbalstwa. Dopiero udostępnienie danych logowania oraz

kodów autoryzacyjnych może być poczytywane jako przejaw rażącego niedbalstwa, szczególnie wówczas gdy z treści wiadomości sms wynika, że kod służy autoryzacji czynności, której uprawniony użytkownik nie zamierza autoryzować, innymi słowy nie zamierza jej przeprowadzić (zob. wyrok Sądu Najwyższego z dnia 15 września 2023 r. w sprawie II CSKP 1013/22). W podobnym stanie faktycznym Sąd Rejonowy Poznań-Stare Miasto w Poznaniu w wyroku z dnia 8 grudnia 2021 r. w sprawie I C 648/20 uznał, że okoliczność udostępnienia na skutek ataku phishingowego oprócz danych logowania do konta bankowości internetowej również kodu autoryzacyjnego przesłanego we wiadomości SMS nie przemawia za rażącym niedbalstwem klienta banku (mimo, że z wiadomości SMS wynikało, że kod autoryzuje transakcję, której klient wcale nie zamierzał zlecać). Powyższe stanowisko, jako zbyt daleko idące, spotkało się jednak w doktrynie ze słuszną krytyką, gdzie wskazuje się, że łączne podanie danych do logowania i kodów autoryzacyjnych trudno traktować jako dopuszczalny błąd, a jest to raczej przejaw rażącego niedbalstwa (vide: Spory między dostawcami usług płatniczych a użytkownikami dotyczące transakcji płatniczych w świetle najnowszego orzecznictwa polskich sądów powszechnych, Bartosz Wyżykowski, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2022, Nr 7, str. 28).

Sąd Okręgowy w pełni podziela wyrażony w orzecznictwie pogląd, że 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). W związku z powyższym na aprobatę zasługuje stwierdzenie, że 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 (tak w wyroku Sądu Okręgowego w Gliwicach - III Wydział Cywilny Odwoławczy z dnia 6 lipca 2022 r. w sprawie III Ca 264/22).

Reasumując, w ocenie Sądu Okręgowego wbrew spoczywającemu na pozwanym ciężarowi dowodu, w niniejszym postępowaniu pozwany nie wykazał, że do nieautoryzowanych transakcji doszło w wyniku będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 ustawy. Pozwany nie udowodnił, że to powódka udostępniła osobom trzecim zarówno dane do logowania do bankowości internetowej jak i kody autoryzujące sporne czynności, a tylko łączne udostępnienie ww. danych można by potraktować w kategorii rażącego niedbalstwa. Wobec powyższego pozwany nie udowodnił, że to płatnik (powódka) ponosi w niniejszej sprawie odpowiedzialność za nieautoryzowane transakcje płatnicze.

Zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika niezwłocznie, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwraca płatnikowi kwotę nieautoryzowanej transakcji płatniczej. Zgłoszenia reklamacji powódka dokonała u pozwanego w dniu 6 lutego 2020 r. (k. 10), a zatem w świetle przytoczonej normy z uwagi na okoliczność, że chodzi o transakcję nieautoryzowaną zwrot środków powinien nastąpić do końca 7 lutego 2020 r., a zatem pozwany pozostaje w opóźnieniu od dnia 8 lutego 2020 r. i od tej daty powódka uprawniona jest do odsetek.

W związku z powyższym, w punkcie I. wyroku, na podstawie art. 386 k.p.c. Sąd Okręgowy zmienił zaskarżony wyrok w punkcie I. w ten tylko sposób, że odsetki ustawowe za opóźnienie od wskazanej tam kwoty 6.000 zł zasądził od dnia 8 lutego 2020 r. do dnia zapłaty, oddalając powództwo w pozostałym zakresie.

W punkcie II. wyrok, na podstawie art. 385 k.p.c. Sąd Okręgowy oddalił apelację w pozostałej części jako bezzasadną.

O kosztach postępowania apelacyjnego Sąd Okręgowy orzekł w punkcie III. i na podstawie art. 98 § 1, § 1^1, § 3 k.p.c. w zw. z art. 99 k.p.c. w zw. z art. 391 § 1 k.p.c. w § 2 pkt 4 i § 10 ust. 1 pkt 1 rozporządzenia Ministra Sprawiedliwości z

dnia 22 października 2015 r. w sprawie opłat za czynności radców prawnych zasądził od pozwanego na rzecz powódki kwotę 900 zł tytułem zwrotu kosztów procesu za instancję odwoławczą z odsetkami ustawowymi za opóźnienie za czas od dnia uprawomocnienia się orzeczenia o kosztach procesu za II instancję do dnia zapłaty.

SSO Jacek Barczewski