Sygn. akt I C 249/16

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 7 września 2017 roku

Sąd Rejonowy dla Łodzi – Śródmieścia w Łodzi, I Wydział Cywilny, w składzie:

Przewodniczący: S.S.R. Bartosz Kasielski

Protokolant: sekretarz sądowy Sylwia Wróblewska

po rozpoznaniu w dniu 24 sierpnia 2017 roku w Łodzi

na rozprawie

sprawy z powództwa M. B. (1)

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

o zapłatę

1. zasądza od (...) Spółki Akcyjnej z siedzibą w W. na rzecz M. B. (1) kwotę 53.205,96 zł (pięćdziesiąt trzy tysiące dwieście pięć złotych 96/100) z ustawowymi odsetkami od dnia 14 lutego 2014 roku do dnia 31 grudnia 2015 roku oraz ustawowymi odsetkami za opóźnienie od dnia 1 stycznia 2016 roku do dnia zapłaty;

2. oddala powództwo w pozostałej części;

3. zasądza od (...) Spółki Akcyjnej z siedzibą w W. na rzecz M. B. (1) kwotę 9.941 zł (dziewięć tysięcy dziewięćset czterdzieści jeden złotych) tytułem kosztów procesu;

4. nakazuje pobrać od (...) Spółki Akcyjnej z siedzibą w W. na rzecz Skarbu Państwa – Sądu Rejonowego dla Łodzi – Śródmieścia w Łodzi kwotę 295,60 zł (dwieście dziewięćdziesiąt pięć złotych 60/100) tytułem nieuiszczonych kosztów sądowych.

Sygnatura akt I C 249/16

UZASADNIENIE

Pozwem z dnia 28 stycznia 2016 roku M. B. (1) wniósł o zasądzenie od (...) Spółki Akcyjnej z siedzibą w W. kwoty 54.476,90 złotych wraz z ustawowymi odsetkami od dnia 14 lutego 2014 roku do dnia zapłaty oraz kosztów procesu, w tym kosztów zastępstwa procesowego, według norm przepisanych.

Żądanie pozwu obejmuje zwrot kwoty nieautoryzowanych transakcji płatniczych dokonanych w dniu 30 stycznia 2014 roku z rachunku bankowego powoda prowadzonego w (...) Spółce Akcyjnej z siedzibą w W..

(pozew k.2 – 9)

Nakazem zapłaty z dnia 24 lutego 2016 roku Sąd Rejonowy dla Łodzi – Śródmieścia w Łodzi orzekł zgodnie z żądaniem pozwu.

(nakaz zapłaty k.77)

W sprzeciwie od nakazu zapłaty (...) Spółka Akcyjna z siedzibą w W. wniosła o oddalenie powództwa oraz przyznanie kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych.

Uzasadniając swoje stanowisko procesowe pozwana wskazała, że kwestionowane transakcje płatnicze były autoryzowane przez M. B. (1), który poprzez skuteczne zalogowanie się do systemu bankowości internetowej używając przyporządkowanego mu identyfikatora i hasła ustanowił definicję odbiorcy zdefiniowanego (I. K.) potwierdzając tą czynność otrzymanym hasłem sms, co w konsekwencji prowadziło do transferu środków pieniężnych na rzecz wskazanej osoby. W ocenie pozwanego brak jest podstaw do przypisania jakiejkolwiek odpowiedzialności po stronie banku za przypadek, w którym dane służące do wykonania transakcji zostały w podstępny sposób uzyskane przez hakerów, tym bardziej, że systemy bezpieczeństwa instytucji bankowej funkcjonowały bez zarzutu. Jednocześnie z ostrożności procesowej (...) Spółka Akcyjna z siedzibą w W. zgłosiła zarzut przyczynienia się powoda do powstania szkody w całości z uwagi na brak zachowania przez M. B. (1) należytej staranności w posługiwaniu się udostępnionym mu instrumentem płatniczym.

(sprzeciw od nakazu zapłaty k.80 – 87)

W toku rozprawy z dnia 24 sierpnia 2017 roku powód sprecyzował, że dochodzi odsetek w wysokości odsetek ustawowych do dnia 31 grudnia 2015 roku oraz w wysokości odsetek ustawowych za opóźnienie od dnia 1 stycznia 2016 roku do dnia zapłaty.

(protokół rozprawy z dnia 24 sierpnia 2017 roku 00:47min k.216)

Sąd Rejonowy ustalił następujący stan faktyczny :

W dniu 3 lipca 2003 roku M. B. (1) zawarł z (...) Bank Spółką Akcyjną z siedzibą w W. (poprzednik prawny (...) Spółki Akcyjnej z siedzibą w W.) umowę o prowadzenie rachunków oszczędnościowych : (...) o numerze (...) oraz (...) o numerze (...).

W związku z zawartą umową bank zobowiązał się do prowadzenia rachunków wskazanych w „Potwierdzeniu otwarcia rachunku" oraz rachunków otwartych w terminie późniejszym na podstawie dyspozycji posiadacza oraz przechowywania środków pieniężnych posiadacza i przeprowadzania na jego zlecenie rozliczeń pieniężnych. Integralną część umowy stanowił Regulamin otwierania i prowadzenia rachunków oszczędnościowych w mBanku (§ 1 umowy).

W myśl § 7 umowy zlecenia przekazywane przez posiadacza, za pośrednictwem poszczególnych kanałów dostępu stanowiły ostateczną i wiążącą mBank podstawę obciążenia rachunku posiadacza oraz uznania rachunku wskazanego w dyspozycji, o ile zostały złożone z zachowaniem warunków niezbędnych do jednoznacznej identyfikacji posiadacza, określonych regulaminie i nie naruszały powszechnie obowiązujących przepisów prawa.

W tym samym dniu M. B. (1), P. B. i M. B. (2) zawarli z (...) Bank Spółką Akcyjną z siedzibą w W. umowę nr (...) o prowadzenie bankowych rachunków bieżących w związku z prowadzoną działalnością gospodarczą (...).P.M. B., przy czym otworzony został rachunek bankowy (...) o numerze (...). Integralną część umowy stanowił Regulamin otwierania i prowadzenia rachunków bieżących w mBanku.

W dniu 9 maja 2005 roku M. B. (1) złożył dyspozycję otwarcia dodatkowego rachunku bankowego (...) o numerze (...).

(umowy o prowadzenie rachunków k.43 – 45, k.49 – 53, potwierdzenia otwarcia rachunków k.46 – 48, k.54 – 55)

Zgodnie z treścią § 2 Regulaminu otwierania i prowadzenia rachunków oszczędnościowych w mBanku na dzień 3 lipca 2003 roku zdefiniowano następujące pojęcia : hasło – ciąg znaków służących do identyfikacji posiadacza rachunku, ustalony w celu zagwarantowania wyłączności dostępu do rachunku i znany jedynie posiadaczowi rachunku (pkt 2), kanał dostępu – sposób komunikacji z mBankiem, obejmujący w szczególności sieć Internet, mLinię, (...),

SMS, bankomat, umożliwiający posiadaczowi rachunku składanie dyspozycji dotyczących rachunku oraz dostęp do informacji i usług bankowych (pkt 4), numer identyfikacyjny – nadawany przez mBank numer służący do identyfikacji posiadacza rachunku (pkt 7), zlecenie stałe - dyspozycja dokonywania powtarzalnych płatności, określająca rachunek wierzyciela, tytuł płatności, stałą kwotę i częstotliwość (pkt 17).

Posiadacz rachunku uzyskiwał dostęp do rachunku za pośrednictwem kanałów dostępu po dokonaniu ich aktywacji uzyskując niepowtarzalny numer identyfikacyjny, który był poufny i nie mógł być ujawniony osobom trzecim. Po uzyskaniu numeru identyfikacyjnego posiadacz rachunku ustalał hasła do kanałów dostępu, które również nie mogły być ujawniane (§ 27 ust. 1 Regulaminu).

Realizacja dyspozycji składanych za pośrednictwem kanałów dostępu wymagała jednoznacznej identyfikacji osoby uprawnionej przy użyciu właściwych dla danego kanału dostępu identyfikatorów wskazanych w tabeli funkcjonalności kanałów dostępu, przy czym mBank zastrzegł sobie prawo odmowy wykonania dyspozycji, gdy zaistniałe okoliczności uzasadniają wątpliwości co do jej autentyczności lub zgodności z przepisami (§ 29 ust. 1 i 2 Regulaminu).

(regulamin otwierania i prowadzenia rachunków oszczędnościowych w mBanku k.135 – 142)

Stosownie do treści § 38 Regulaminu otwierania i prowadzenia bankowych rachunków dla osób fizycznych w ramach bankowości detalicznej (...) Spółki Akcyjnej (obowiązującego od dnia 25 stycznia 2014 roku) zabezpieczeniu bezpieczeństwa dyspozycji składanych do rachunku służyły identyfikacja posiadacza rachunku oraz autoryzacja transakcji płatniczych przez płatnika oraz potwierdzenie złożenia dyspozycji przez posiadacza rachunku. Identyfikator, hasła do kanałów dostępu oraz hasła jednorazowe przeznaczone były wyłącznie dla posiadacza rachunku, nie mogły być ujawnione w żadnej formie, treści ani postaci osobom trzecim, w tym członkom rodziny, nie były znane organom ani pracownikom banku, jak również innym podmiotom działającym na rzecz zlecenie banku, a nadto były nadawane z zachowaniem procedur zapewniających zachowanie ich w poufności z wykorzystaniem programów komputerowych, a uzyskanie informacji o jednym z nich nie pozwalało na równoczesne uzyskanie informacji o jednym z nich. Posiadacz rachunku zobowiązany był nadto do podjęcia niezbędnych środków służących zapobieżeniu naruszenia indywidualnych zabezpieczeń identyfikatora, hasła oraz haseł jednorazowych, w szczególności zaś zobowiązany był do ich przechowywania z zachowaniem należytej staranności.

Posiadacz rachunku zobowiązany był do niezwłocznego zgłoszenia do banku stwierdzenia utraty, kradzieży, przywłaszczenia, nieprawidłowego użycia lub dostępu identyfikatora, hasła do kanału dostępu lub hasła jednorazowego, zaś w przypadku utraty lub wystąpienia podejrzeń o możliwość wejścia osób trzecich w posiadanie hasła do kanału dostępu niezwłocznej zmiany hasła do kanału dostępu lub zablokowania kanału dostępu za pośrednictwem BOK lub w placówce banku (§ 39 ust. 1 i 3 regulaminu). W myśl § 41 ust. 1 Regulaminu posiadacz rachunku zobowiązany był do należytego zabezpieczenia narzędzi i urządzeń, z których korzysta w celu uzyskania dostępu do rachunku, w szczególności nie omijania fabrycznych zabezpieczeń urządzeń telekomunikacyjnych, zainstalowania na urządzeniu legalnego oprogramowania systemowego oraz antywirusowego, pobrania aplikacji mobilnej w sposób wskazany przez bank oraz dokonywania aktualizacji zainstalowanego na urządzeniu legalnego oprogramowania systemowego oraz antywirusowego.

Zapisy tożsamej treści zostały opisane w § 41, 42 i 44 regulaminu otwierania i prowadzenia rachunków bieżących dla firm w ramach bankowości detalicznej (...) Spółki Akcyjnej (obowiązującego od dnia 25 stycznia 2014 roku).

(regulamin otwierania i prowadzenia bankowych rachunków dla osób fizycznych k.99 – 101, regulamin otwierania i prowadzenia rachunków bieżących dla firm w ramach bankowości detalicznej k.102 – 103)

M. B. (1) korzystał przez okres około 10 lat głównie z rachunków bankowych indywidualnych prowadzonych przez (...) Spółkę Akcyjną z siedzibą w W.. Konto firmowe – (...) (65 1140 ...) wykorzystywane było głównie do czasu zrezygnowania z prowadzenia wspólnej działalności gospodarczej przez jego synów P. B. i M. B. (2), co miało miejsce

w 2004 roku. Każda z osób posiadających dostęp do konta biznesowego dysponowała przypisanymi sobie danymi pozwalającymi na indywidualny dostęp do rachunku. M. B. (1), P. B. i M. B. (2) nie przekazywali sobie tych danych.

M. B. (1) przez cały okres korzystania z usług banku posiadał dostęp internetowy do prowadzonych rachunków, co wymagało podania numeru identyfikacyjnego oraz hasła. Jednocześnie autoryzacja poszczególnych transakcji, w tym również ustanowienie tzw. odbiorcy zdefiniowanego wymagała potwierdzenia czynności kodem sms, zawierającym unikatowy (...), uzyskiwanym każdorazowo na wskazany numer telefonu komórkowego.

Transakcje płatnicze realizowane w ramach konta indywidualnego (...) (35 1140 ...) dotyczyły przeważnie przelewów kwot o niskiej wartości (nieprzekraczającej kilku tysięcy złotych).

M. B. (1) nie udostępniał nigdy żadnej osobie numeru identyfikacyjnego i hasła do kanałów dostępu. Mężczyzna nie korzystał z aplikacji mobilnej oferowanej przez bank. Do systemu transakcyjnego banku (...) uzyskiwał dostęp z komputera domowego i firmowego, które posiadały legalne oprogramowanie systemowe W. (...) oraz program antywirusowy A., przy czym usługa internetowa dostarczana była przez firmę (...). W ramach korzystania z Internetu mężczyzna używał routera marki E.. M. B. (1) nigdy nie wykonywał transakcji w trybie S.. Nadto starał się zapoznawać z informacjami, w tym dotyczącymi systemów bezpieczeństwa, przedstawianymi przez mBank na stronie logowania do serwisu transakcyjnego.

(dowód z przesłuchania powoda – protokół rozprawy z dnia 7 lipca 2016 roku 6:07min – 31:26min k.148 – 151 w zw. z protokołem rozprawy z dnia 24 sierpnia 2017 roku 3:10min k.216, zeznania świadka P. B. – protokół rozprawy z dnia 4 października 2016 roku 9:21min – 29:40min k.164 – 165, zeznania świadka M. B. (2) – protokół rozprawy z dnia 4 października 2016 roku 30:35min – 54:38min, faktura VAT k.72)

W dniu 30 stycznia 2014 roku około godziny 14:00 M. B. (1) zamierzał dokonać płatności z tytułu opłat za gaz na rzecz (...) Spółki Akcyjnej, który był zapisany w systemie transakcyjnym jako odbiorca zdefiniowany. W tym celu mężczyzna wprowadził niezbędne dane identyfikujące (numer identyfikacyjny i hasło) na witrynie internetowej, która odpowiadała swym obrazem, zestawieniem detali i wyglądem stronie systemu transakcyjnego mBanku. Mężczyzna wpisał dane opisujące przelew (nr faktury). Po chwili M. B. (1) otrzymał na swój numer telefonu (507-507-055) sms o treści „! Operacja nr 1 z dn. 30-01-2014 Definicja odbiorcy z rach: ... (...) na rach: 4810... (...) hasło : *** mBank. Mężczyzna wypełnił wymagane pole w ramach widocznej strony internetowej podanym kodem SMS zgodnie z wyświetlonym poleceniem, a następnie wyłączył komputer i pojechał do pracy.

(dowód z przesłuchania powoda – protokół rozprawy z dnia 7 lipca 2016 roku 15:13min – 16:56min k.149 – 150, 54:49min k.152, 58:12min – k.153 w zw. z protokołem rozprawy z dnia 24 sierpnia 2017 roku 3:10min k.216, zeznania świadka P. B. – protokół rozprawy z dnia 4 października 2016 roku 27:59min – 29:01min k.165, treść wiadomości SMS k.113)

W dniu 30 stycznia 2014 roku wykonane zostały transakcje środków pieniężnych w kwocie 2.974 złotych z konta (...) (35 1140 ...) na konto (...) (65 1140 ...) oraz w kwocie 52.004 złotych z konta (...) (38 1140 ...) na konto (...) (65 1140 ...). Następnie z konta (...) (65 1140 ...) wykonane zostały dwie transakcje przelewu środków pieniężnych w trybie S. w kwotach 26.127,30 złotych oraz 28.279,60 złotych na rachunek nr (...) prowadzony na rzecz osoby o danych I. K.. Koszt każdej transakcji w trybie S. wyniósł po 35 złotych, łącznie 70 złotych.

(elektroniczne zestawienia operacji k.56 – 59)

W godzinach wieczornych dnia 30 stycznia 2014 roku M. B. (1) ponownie zalogował się do internetowego systemu transakcyjnego banku i stwierdził brak środków na kontach bankowych, co sygnalizował czerwony kolor (debet). Z uwagi na dezorientację co do zaistniałego stanu rzeczy mężczyzna udał się do swojego syna P. B., zamieszkującego w tym samym budynku. M. B. (1) wykorzystał telefon komórkowy syna celem ponownego dostępu do systemu bankowego i potwierdził brak środków pieniężnych w wysokości kilkudziesięciu tysięcy złotych. Mężczyzna

natychmiast skontaktował się z pracownikami banku poprzez m-linię, co skutkowało zablokowaniem internetowego kanału dostępu.

Po zdarzeniu komputery używane przez M. B. (1) zostały sprawdzone przez jego synów przy użyciu programów antywirusowych A. i A., przy czym nie wykryto na nich żadnego złośliwego oprogramowania. Jednocześnie M. B. (2) ustalił, że numer (...) znajdujący się na komputerze jego ojca jest podatny na przełamywanie zabezpieczeń w związku z używaniem routera marki E..

(dowód z przesłuchania powoda – protokół rozprawy z dnia 7 lipca 2016 roku 17:15min – 17:45min k.150 w zw. z protokołem rozprawy z dnia 24 sierpnia 2017 roku 3:10min k.216, zeznania świadka P. B. – protokół rozprawy z dnia 4 października 2016 roku 6:31min – 8:46min k.164, zeznania świadka M. B. (2) – protokół rozprawy z dnia 4 października 2016 roku 50:21min – 53:41min k.167)

W okresie od dnia 28 stycznia 2014 roku do dnia 29 stycznia 2014 roku logowania do internetowego systemu transakcyjnego mBanku następowało z komputerów posiadających systemy operacyjne W. (...) i W. (...), przy wykorzystaniu przeglądarki internetowej Chrome i adresu IP przyporządkowanego przez operatora N..

W dniu 30 stycznia 2014 roku dostęp do systemu bankowości internetowej nastąpił z komputera z systemem operacyjnym W. (...) przy użyciu przeglądarki internetowej Internet E. oraz adresu IP przyporządkowanego przez operatora (...) in (...), przy czym klasa adresowa IP podlegała w tym przypadku domenie hostingowej hosteam.pl.

(...) hostingowy z własną klasą adresową to serwer, na którym dowolne osoby mogą zestawić własną stronę internetową np. lustrzaną kopię strony internetowej mBanku, która jest na tyle dobrze spreparowana, że potencjalny posiadacz rachunku bankowego nie ma świadomości, że nie korzysta z właściwej strony internetowej banku. W ramach tak przygotowanej strony możliwym jest zainstalowanie kwerend zaczytujących loginy i hasła, a także generujących dodatkowe aplety wymuszające wprowadzenie przez posiadacza rachunku danych niezbędnych do autoryzowania transakcji, czy też ustanowienia odbiorcy zdefiniowanego.

W przypadku routerów marki E. osoba trzecia, działając z zewnątrz, może za pomocą komendy z przeglądarki internetowej pobrać z routera bakcup konfiguracji, a następnie zdekodować uzyskane dane celem poznania loginu i hasła administracyjnego urządzenia, co pozwala na bezproblemowy dostęp do routera i wprowadzania danych innych serwerów (...). Identyfikacja użytkownika korzystającego z tego typu routera była niezwykle prosta i sprowadzała się do napisania skryptu przeszukującego adresy IP.

Router jako urządzenie pośredniczące w wymianie ruchu internetowego pomiędzy komputerem, a siecią internetową jest tzw. urządzeniem wykonującym przekserowanie nazw domenowych na konkretne adresy IP. Osoba wprowadzająca w przeglądarce internetowej adres strony banku za pomocą routera, który przerzuca serwery (...) do klientów, zamienia adres strony wpisany w sposób czytelny dla użytkownika na adres IP konkretnego hosta. Router wie, jaki jest adres IP po wpisaniu wybranej strony, bo komunikuje się kaskadowo z kolejnymi serwerami (...) celem poznania odpowiedzi na to zapytanie. Z kolei serwery (...) w zakresie konfiguracji dostępu do sieci I. standardowo są dostarczane przez operatorów telekomunikacyjnych wraz z automatyczną konfiguracją pobieraną z serwera operatora, jednakże każdy z abonentów może ingerować w te ustawienia i wpisać sobie inne serwery (...).

Wprowadzenie innych adresów serwerów (...) w dniu 30 stycznia 2014 roku skutkowało tym, że w chwili wpisania w przeglądarce internetowej adresu strony banku, router odpytywał wskazany adres (...), a ten podawał w adresie zwrotnym podstawioną stronę internetową banku, lecz nie kierował bezpośrednio do prawdziwej. Tym samym M. B. (1) uzyskał odbicie lustrzane dobrze spreparowanej przez osoby trzecie strony banku i w jej ramach wykonywał operacje związane z systemem bankowym, który traktował za wiarygodny.

Podstawiony przez osoby trzecie serwer (...) imitujący stronę banku pozwolił osobom trzecim na uzyskanie danych numeru identyfikującego i hasła, które M. B. (1) wprowadzał celem uzyskania dostępu do systemu bankowości elektronicznej. W dalszej kolejności za pomocą wygenerowania komunikatów żądających od użytkownika

wprowadzenia hasła jednorazowego SMS mężczyzna wprowadził uzyskany kod (...), co umożliwiło ustanowienie odbiorcy zdefiniowanego. Najprawdopodobniej podstawiona strona banku imitowała konieczność ponownego zdefiniowania jako odbiorcy (...), gdy w rzeczywistości operacja dotyczyła nowego odbiorcy o danych I. K.. Zamierzony przez M. B. (1) przelew środków pieniężnych tytułem opłaty za gaz nastąpił o godzinie 14:02:27, a wylogowanie z systemu bankowości internetowej o godzinie 14:02:44. Wszelkie dane dotyczące logowania, a następnie wprowadzenia hasła SMS wprowadzane były na podstawionej usłudze hostingowej, a następnie forwardowanej do rzeczywistej strony mBanku, przy czym kopia danych (w tym numer identyfikacyjny, hasło i kod SMS) pozostawały na serwerze (...) podstawionym M. B. (1) przez osoby trzecie.

Kolejne logowanie do systemu bankowości internetowej nastąpiło o godzinie 14:43:31 z komputera posiadającego system operacyjny W. (...) przy użyciu przeglądarki internetowej Internet E. i adresu IP przyporządkowanego przez operatora (...) Sp. z o.o. na tą chwilę T. S. (zamieszkałemu w miejscowości P.). Osoba korzystająca z tego adresu dokonała wewnętrznych przelewów między rachunkami bankowymi M. B. (1) (14:46:13 – kwota 52.004 złotych oraz 14:46:41 – kwota 2.974 złotych) gromadząc je na rachunku (...) (65 1140...), z którego następnie wykonano dwie transakcje na kwoty 26.127,30 złotych (14:47:31) oraz 28.279,60 złotych (14:48:14) na rachunek bankowy odbiorcy zdefiniowanego – I. K.. W. z systemu miało miejsce o godzinie 14:52:20. W późniejszym okresie ten sam użytkownik dokonał ponownego zalogowania do systemu o godzinach 15:57:53, 16:51:52, 17:15:08 oraz 18:57:00.

Sporne transakcje wykonane zostały tuż przed godziną 15:00 tj. graniczną godziną wykonywania operacji typu S.. W dacie ich realizacji bank podejmował kroki konsolidacyjne, co wiązało się z licznymi komunikatami na stronach internetowych i zmianą struktury. Okoliczności te z jednej strony uśmierzały czujność klientów banku, a z drugiej mogły wpływać na zmniejszoną skuteczność funkcjonujących na co dzień wzorców zabezpieczeń.

(...) antyfraudowy według zdefiniowanych reguł selekcjonuje automatycznie te zdarzenia dotyczące transferu gotówki, które z danego klucza muszą zostać zweryfikowane jako podejrzane. W styczniu 2014 roku system ten był obsługiwany przez pracowników etatowych banku, którzy pracowali w systemie jednozmianowym w godzinach 9 – 17. Dopiero od 2015 roku wprowadzono nadzór całodobowy. (...) antyfraudowy nigdy nie weryfikował jako alertu zdefiniowania odbiorcy zaufanego, gdyż ta operacja nie jest związana z transferem gotówki.

(opinia biegłego z zakresu informatyki k.175 – 200, zeznania świadka J. S. – protokół rozprawy z dnia 7 lipca 2016 roku 40:52min – 1h37:23min k.152 – 155, zestawienie logowań autoryzacyjnych – k.114)

Bank opublikował na swojej stronie internetowej ostrzeżenie o potencjalnym zagrożeniu ze strony routerów i możliwości zamiany adresów serwerów (...) w dniu 7 lutego 2014 roku.

(opinia biegłego z zakresu informatyki k.193 – 195)

Dostęp do systemu transakcyjnego mBanku wymaga wskazania prawidłowego numeru identyfikacyjnego oraz hasła zdefiniowanego przez posiadacza rachunku. Bank posiada wiedzę jedynie o numerze identyfikacyjnym przyporządkowanym do danego posiadacza rachunku, przy czym nie jest możliwe zweryfikowanie po zalogowaniu, czy w istocie czynności tej dokonała osoba będąca klientem banku. W 2014 roku żaden z pracowników banku nie miał dostępu do treści wiadomości sms, zawierającej kod (...) do autoryzacji czynności.

W banku funkcjonował system tzw. alertu fraudowego, w ramach którego poszczególne osoby wykonują manualne czynności mogące prowadzić do zablokowania transakcji, przy czym taka reakcja w przypadku przelewu typu S. jest mało prawdopodobna. Transakcja budząca wątpliwości winna skutkować kontaktem z posiadaczem rachunku w trybie wiadomości sms lub e-mail bądź rozmową telefoniczną.

Co do zasady pracownicy banku nie są w stanie ustalić miejsca, z którego następuje logowanie do systemu transakcyjnego z uwagi na przyporządkowanie dynamicznych numerów IP przez dostawcę Internetu. Okoliczność ta uniemożliwia skuteczne działanie systemu antyfraudowego wobec liczby klientów banku oraz liczne zmiany numerów

IP. Próba stworzenia systemu opartego na kilku warunkach np. zmienny adres IP, wysoka kwota transakcji, brak uprzednich operacji na taką kwotę wymagałaby skorzystania z systemu behawioralnego budującego mapę zachowań klienta i reagującego na wszelkie odstępstwa.

Transakcje pomiędzy rachunkami bankowymi tego samego posiadacza nie wymagają dodatkowego potwierdzenia. Utworzenie odbiorcy zdefiniowanego musi zostać poprzedzona autoryzacją poprzez jednorazowe hasło sms. Po jego wprowadzeniu i skutecznym ustanowieniu odbiorcy bank nie wymagał dalszych potwierdzeń przelewów do tak zdefiniowanego odbiorcy. Ustawienia te występują jako domyślna reguła, która może być zmieniona na indywidualne życzenie posiadacza rachunku.

(zeznania świadka J. S. – protokół rozprawy z dnia 7 lipca 2016 roku 1h40:13min – 2h22:11min k.155 – 157)

M. B. (1), P. B. i M. B. (2) nie znają osób o danych I. K. i T. S., nie widzieli ich nigdy w życiu i nie podejmowali z nimi jakichkolwiek kontaktów.

(dowód z przesłuchania powoda – protokół rozprawy z dnia 7 lipca 2016 roku 21:40min k.150 w zw. z protokołem rozprawy z dnia 24 sierpnia 2017 roku 3:10min k.216, zeznania świadka P. B. – protokół rozprawy z dnia 4 października 2016 roku 16:45min k.165, zeznania świadka M. B. (2) – protokół rozprawy z dnia 4 października 2016 roku 38:39min k.166)

W okresie od dnia 19 listopada 2004 roku do dnia 30 stycznia 2014 roku z rachunku bankowego (...) (65 1140 ...) nie były wykonywane transakcje wychodzące o wartości kilkunastu tysięcy złotych. Ostatnia transakcja tego typu tj. o wartości 32.043,30 złotych została wykonana w dniu 19 listopada 2004 roku na rzecz Drukarni (...) tytułem opłaty za fakturę nr (...).

(elektroniczne zestawienia operacji k.60)

W dniu 31 stycznia 2014 roku M. B. (1) zgłosił w Komendzie Rejonowej Policji w W. zawiadomienie o dokonaniu na jego szkodę nieuprawnionej transakcji płatniczej z dnia 30 stycznia 2014 roku na łączną kwotę 54.406,90 złotych.

Postanowieniem z dnia 29 sierpnia 2014 roku Prokuratura Rejonowa W. – Ż. w W. umorzyła dochodzenie w sprawie 4 Ds. 202/14/III dotyczącej dokonania w dniu 30 stycznia 2014 roku przez nieznanego sprawcę działającego w nieustalonym miejscu poprzez sieć Internet w celu osiągnięcia korzyści majątkowej nieuprawnionych przelewów z rachunków bankowych należących do M. B. (1), prowadzonych przez (...) Spółkę Akcyjną z siedzibą w W. tj. o czyn z art. 287 § 1 k.k. wobec niewykrycia sprawcy czynu zabronionego.

(poświadczenie k.61, postanowienie o umorzeniu dochodzenia k.62 – 64)

Pismem z dnia 5 lutego 2014 roku M. B. (1) zwrócił się do mBanku o udostępnienie informacji związanych z utratą środków pieniężnych zgromadzonych na rachunkach bankowych. Pismem z dnia 18 grudnia 2014 roku mBank odmówił uwzględnienia jakichkolwiek roszczeń wskazując na autoryzację spornych przelewów. W odwołaniu z dnia 7 stycznia 2015 roku M. B. (1) wniósł o ponowne rozpatrzenie jego sprawy i zaspokojenie zgłoszonych roszczeń.

(pisma z dnia 5 lutego 2014 roku, 18 grudnia 2014 roku oraz 7 stycznia 2015 roku k.66 – 71)

Powyższy stan faktyczny Sąd ustalił na podstawie zgromadzonego w sprawie materiału dowodowego, w szczególności depozycji powoda, zeznań świadków J. S., M. B. (2), P. B., złożonych przez strony dokumentów, a także opinii biegłego z zakresu informatyki.

Złożona ekspertyza była rzetelna, konsekwentna oraz szczegółowo odpowiadała na zakreśloną tezę dowodową, w tym przedstawiała model działania osób trzecich skutkujących wyprowadzeniem środków pieniężnych z rachunków bankowych powoda. Uwzględniając brak zastrzeżeń stron co do jej merytorycznego zakresu związanego z opisem

zagadnień informatycznych oraz odtworzenia dokonywanych operacji w dniu 30 stycznia 2014 roku, a także wiedzę eksperta z powierzonej mu dziedziny Sąd nie znalazł podstaw do pominięcia jej ostatecznych konkluzji w ramach rekonstrukcji stanu faktycznego. Jedynie na marginesie należy zaznaczyć, że nie były brane pod uwagę wszelkie uwagi biegłego, które wykraczały poza zlecone mu zadanie, w szczególności wyrażane przez eksperta tezy odnośnie legitymacji biernej strony pozwanej oraz oceny zachowania M. B. (1). Warto wskazać, że ekspertyza biegłego ogranicza się do wiadomości specjalnych, które w tej konkretnej sprawie sprowadzały się do zagadnień natury informatycznej. Z kolei rolą Sądu pozostaje ocena ustalonego stanu faktycznego i zastosowanie właściwych przepisów prawa. W tym kontekście poszczególne wnioski zawarte w opinii nie mogły być brane pod uwagę, jako wykraczające poza zlecenie dla eksperta i ingerujące w samodzielność orzeczniczą Sądu.

Sąd oddalił przy tym wniosek strony pozwanej o zlecenie biegłemu analizy skuteczności zabezpieczeń systemu informatycznego stosowanych przez bank w styczniu 2014 roku, a także żądanie powoda o zobowiązanie banku do przedłożenia informacji dotyczącej nieautoryzowanych transakcji w okresie od lipca 2013 roku do lipca 2014 roku. Złożone wnioski dowodowe nie miały znaczenia dla rozstrzygnięcia niniejszej sprawy, której przedmiotem pozostawała ocena, czy sporne transakcje z dnia 30 stycznia 2014 roku były autoryzowane przez M. B. (1).

Sąd Rejonowy zważył, co następuje:

Powództwo zasługiwało na uwzględnienie w przeważającej części.

W niniejszej sprawie bezspornym pozostawały fakty łączących strony umów rachunków bankowych oraz dokonania w dniu 30 stycznia 2014 roku z rachunku bankowego M. B. (1) dwóch przelewów środków pieniężnych w łącznej kwocie 54.406,90 złotych na rachunek bankowy należący do osoby o danych I. K.. Osią sporu pozostaje natomiast ocena, czy przedmiotowe transakcje były autoryzowane przez powoda, czy też miała miejsce nieautoryzowana transakcja płatnicza, której ryzyko dokonania obciąża bank.

Stosownie do treści art. 725 k.c. przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych. W myśl zaś art. 726 k.c. na banku spoczywa obowiązek zwrotu wolnych środków pieniężnych na każde żądanie, chyba że umowa uzależnia obowiązek zwrotu od wypowiedzenia.

Zapewnienie bezpieczeństwa depozytów jest jednym z najistotniejszych obowiązków banku, a sposób jego wykonywania jest najbardziej wymierną podstawą oceny jego wiarygodności, w związku z czym wszelkie próby interpretacji przez banki postanowień zawartych w stosowanych przez nie wzorcach umownych, zmierzające do zaniżania standardów bezpieczeństwa powierzonych bankowi środków pieniężnych, powinny być oceniane jako zachowania sprzeczne z dobrymi obyczajami i celem umowy rachunku bankowego (por. wyrok SN z dnia 14 kwietnia 2003 roku, I CKN 308/01, Legalis nr 61218).

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

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

instrumentu płatniczego, którym jest zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego (art. 2 pkt 10 u.u.p.).

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

Stosownie do treści art. 46 ust. 1 u.u.p. w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku, gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. W myśl zaś art. 45 ust. 1 u.u.p. ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Należy mieć jednak na uwadze, że wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 (art. 45 ust. 2 u.u.p.).

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

W tym miejscu należy wskazać, że implementowana do porządku krajowego dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 roku w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, (...), (...) i (...) i uchylająca dyrektywę 97/5/WE (Dz.U.UE. L 319/1) zawiera sformułowanie transakcja „autentykowana", podczas gdy polski ustawodawca posługuje się zwrotem transakcja „autoryzowana". Warto jednak podkreślić, że zgodnie z art. 288 ust. 3 Traktatu o Funkcjonowaniu Unii Europejskiej (w dalszej części (...)) dyrektywa wiąże każde Państwo Członkowskie, do którego jest kierowana, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawia jednak organom krajowym swobodę wyboru formy i środków. Jednym z celów Dyrektywy 2007/64/WE z dnia 13 listopada 2007 roku było zmniejszenie ryzyka i konsekwencji nieautoryzowanych lub nieprawidłowo wykonanych usług płatniczych z punktu widzenia użytkownika usług płatniczych, którym w przeważającej części przypadków pozostaje konsument. I tak w treści preambuły do przedmiotowej Dyrektywy ustawodawca europejski zaznaczył m.in., że ocena ewentualnego zaniedbania ze strony użytkownika usług płatniczych winna uwzględnić wszystkie okoliczności. Oczywistość i stopień domniemanego zaniedbania powinien ocenić sąd zgodnie z prawem krajowym. Warunki umowne dotyczące wydania i korzystania z instrumentu płatniczego, których skutkiem byłoby zwiększenia ciężaru dowodu spoczywającego na konsumencie lub zmniejszenie ciężaru dowodu spoczywającego na wydawcy, powinny być uznane za nieważne (pkt 33 preambuły). Nadto Państwa członkowskie powinny mieć możliwość ustalenia zasad mniej rygorystycznych niż zasady określone powyżej w celu utrzymania istniejącego poziomu ochrony konsumentów i propagowania zaufania do bezpiecznego korzystania z elektronicznych instrumentów płatniczych. Fakt, że różne instrumenty płatnicze wiążą się z różnymi

rodzajami ryzyka, powinien być odpowiednio uwzględniany, co powinno pomóc w propagowaniu wydawania bezpieczniejszych instrumentów. Powinno zezwolić się państwom członkowskim na ograniczenie lub zupełne wyłączenie odpowiedzialności płatnika, z wyjątkiem sytuacji, w których płatnik działał w nieuczciwych zamiarach (pkt 34 preambuły). Istotnie w angielskojęzycznej wersji przedmiotowej Dyrektywy, a mianowicie art. 59 ust. 1 użyto sformułowań „authorised" oraz „authenticated", przy czym w ust. 2 tego przepisu użyto wyłącznie zwrotu „authorised". Zarówno w polskojęzycznej, jak i angielskojęzycznej wersji dokumentu bezspornie jednak przyjęto, że samo użycie instrumentu płatniczego niekoniecznie jest wystarczające do udowodnienia, że transakcja płatnicza została przez płatnika usług płatniczych autoryzowana (ust.2). Co więcej, gdyby nawet próbować forsować tezę o niewłaściwym tłumaczeniu zwrotu „authenticated" na gruncie art. 59 ust. 1, nie można stracić z pola widzenia, że implementacja Dyrektywy została dokonana w ramach ustawy o usługach płatniczych, na gruncie której ustawodawca polski był w pełni uprawniony do zastosowania bardziej rygorystycznych zapisów mających realizować cel aktu prawnego Unii Europejskiej. Innym słowy harmonizacja przepisów na poziomie Państw Członkowskich jest instrumentem realizującym podstawowy cel Dyrektywy, przy czym każde z Państw Członkowskich dysponuje swobodą formy i środków, które mają ten rezultat uzyskać. O ile uzasadnionym pozostawałoby powoływanie się na brak realizacji tego celu w ramach implementacji lub osiągnięcia rezultatu nieodpowiadającego wyznaczonym standardom, o tyle chybioną pozostaje argumentacja o zastosowaniu środków bardziej restrykcyjnych niż przewidziane, w szczególności w kontekście treści preambuły oraz prokonsumenckiej wykładni przepisów w relacjach konsumenta z profesjonalistą.

Przenosząc treść powyższych regulacji na płaszczyznę przedmiotowej sprawy rozstrzygnięciu podlega kwestia, czy sporne transakcje płatnicze były autoryzowane przez M. B. (1).

Zgromadzony materiał dowodowy prowadzi do wniosku, że w dniu 30 stycznia 2014 roku nieustalona osoba wykorzystująca luki w systemie zabezpieczeń routera używanego przez M. B. (1) uzyskała bez jego wiedzy informacje dotyczące numeru identyfikacyjnego i hasła, które służyły do skutecznego dostępu do internetowego systemu transakcyjnego mBanku. Jednocześnie poprzez zamianę adresów (...) mężczyzna pozostawał w pełnym przekonaniu, że zalogował się do właściwej strony internetowej banku, podczas gdy w rzeczywistości przedstawiona została mu łudząco podobna witryna, z której wszelkie wprowadzane dane były przejmowane (kopiowane) przez osobę trzecią, a następnie forwardowane do prawdziwego systemu transakcyjnego. Z uwagi na brak zabezpieczenia używanego przez powoda komputera i poddania go analizie ze strony organów ścigania nie jest możliwe ustalenie faktycznej treści komunikatu, który skutkował koniecznością wprowadzenia jednorazowego hasła otrzymanego drogą sms. Mogło to być zarówno żądanie dodatkowego potwierdzenia wykonywanej transakcji, czy też wymuszenie ponownego ustanowienia (...) jako odbiorcy zdefiniowanego. Niemniej jednak polecenie to było na tyle wiarygodne dla M. B. (1), że spowodowało podstępne wyłudzenie od klienta banku wprowadzenia hasła jednorazowego prowadzącego do dokonania czynności odbiegającej od rzeczywistej woli posiadacza rachunku bankowego. W konsekwencji doszło do ustanowienia nowego odbiorcy zdefiniowanego – osoby o danych I. K., a następnie wykonania dwóch spornych przelewów na rzecz tego podmiotu.

Uwzględniając powyższe Sąd stwierdził brak podstaw do uznania, że transakcje płatnicze z dnia 30 stycznia 2014 roku były autoryzowane przez M. B. (1). Sam fakt prawidłowego logowania do systemu bankowości internetowej mBanku przy użyciu prawidłowej nazwy użytkownika oraz hasła, a następnie ustanowienie odbiorcy zaufanego po wykorzystaniu wysłanej wiadomości tekstowej SMS nie przesądza jeszcze, że wykonane w tym dniu transakcje była autoryzowane przez powoda.

Po pierwsze, w żadnej mierze nie zostało udowodnione, że powód akceptował w jakikolwiek sposób dokonanie przelewów na rzecz osoby o danych I. K., czy też miał zamiar przeprowadzić transakcję, której beneficjentem byłyby właśnie ten podmiot.

Po wtóre, M. B. (1) nigdy nie udostępniał żadnej osobie danych uprawniających do korzystania z internetowego systemu transakcyjnego banku. Powód zgodnie z treścią łączącej go z pozwanym umowy, regulaminu, jak również normą art. 42 ust. 2 u.u.p. przechowywał dane związane z instrumentem płatniczym z zachowaniem należytej

ostrożności. Nadto używany przez niego sprzęt komputerowy wyposażony był w legalne oprogramowanie systemowe oraz antywirusowe.

Po trzecie, powód zapoznawał się z treścią komunikatów i ostrzeżeń prezentowanych na witrynie transakcyjnej banku. Informacja o potencjalnym zagrożeniu ze strony routerów została jednak przedstawiona posiadaczom rachunków dopiero w dniu 7 lutego 2014 roku, a więc tydzień po dokonaniu spornych przelewów.

Po czwarte, M. B. (1), ani żaden z jego synów nie zna i nigdy nie kontaktował się z osobami o danych I. K. (odbiorca zdefiniowany), czy T. S. (posiadacz komputera, z którego adresu IP dokonywano spornych transakcji).

Po piąte, z samego faktu ustanowienia nowego odbiorcy zdefiniowanego nie można wyciągać wniosków prowadzących do uznania transakcji za autoryzowane. Bezspornym pozostaje fakt, że dokonanie tego typu operacji wymagało autoryzacji poprzez wprowadzenie hasła jednorazowego sms. Niekwestionowaną jest również okoliczność, że powód otrzymał wiadomość sms i wprowadził do odpowiedniego pola w ramach witryny internetowej jego treść (hasło jednorazowe). Trudno jednak przyjąć, aby intencją M. B. (1) pozostawało dokonanie tego typu operacji, skoro mężczyzna miał zamiar opłacić stosowną fakturę tytułem opłaty za gaz. Przyjęcie odmiennej koncepcji i uznanie, że powód w istocie autoryzował tą czynność nie prowadzi jednak do automatycznego stwierdzenia, że autoryzował on również przelewy na rzecz nieznanej mu osoby. Strona pozwana nie przedłożyła żadnych dokumentów, które opisywałyby proces ustanowienia odbiorcy zdefiniowanego, a także skutki związane z taką czynnością. Jedynie z dostępnego materiału dowodowego w postaci zeznań świadków należy wnioskować, że ustanowienie odbiorcy zdefiniowanego wymagało autoryzacji jednorazowym hasłem SMS, przy czym z uwagi na domyślną opcję stosowaną przez bank (a w rzeczywistości z góry narzuconą) wszelkie transakcje środków na rzecz takiego podmiotu nie wymagały dalszej autoryzacji. Nie sposób stwierdzić, na jakiej podstawie funkcjonowała ta „domyślna opcja", czy była elementem łączącego strony stosunku prawnego (umowa o prowadzenie rachunku bankowego, regulamin), a przede wszystkim, czy była akceptowana przez posiadacza rachunku (w tym przypadku powoda) i czy miał on świadomość takiego funkcjonowania systemu transakcyjnego. Próba uzasadnienia tej reguły jej funkcjonalnością i zapewnieniem wygody klientom banku nie znajduje racjonalnego uzasadnienia w kontekście obowiązku instytucji finansowej w zakresie zapewnienia bezpieczeństwa depozytów. Ustanowienie odbiorcy zdefiniowanego sprowadzało się do określenia podstawowych danych tego podmiotu, przy czym nie wymagało określenia wysokości planowanej transakcji (w odróżnieniu chociażby o tzw. zleceń stałych). W takich warunkach trudno jest przyjąć, aby szczególną niedogodność dla posiadacza rachunku stanowił obowiązek autoryzowania opcji wykonywania przelewów na rzecz odbiorcy zdefiniowanego bez konieczności ich potwierdzania w przyszłości. Czynność ta ograniczałaby się bowiem jedynie do wprowadzenia dwóch haseł jednorazowych (ustanowienie odbiorcy oraz wyłączenie każdorazowej autoryzacji przelewu na jego rzecz), które przy ich właściwym opisie w ramach wiadomości SMS, nie pozostawiałyby wątpliwości co do rzeczywistej woli posiadacza rachunku. W realiach niniejszej sprawy stosowana przez bank domyślna opcja pozbawiała powoda realnej możliwości autoryzacji transakcji na konkretną sumę pieniężną, a z drugiej strony kreowała dla instytucji finansowej podstawę do argumentacji zmierzającej każdorazowo do uwolnienia się od odpowiedzialności, czego nie można w żadnej mierze zaakceptować.

Uwzględniając powyższe argumenty należy ponownie odnieść się do treści art. 45 ust. 2 u.u.p. należy podkreślić, że ryzyko zarejestrowanego użycia instrumentu płatniczego nieautoryzowanego przez klienta obciąża bank, o ile tylko klient nie doprowadził do nieautoryzowanej transakcji umyślnie albo na skutek rażącego niedbalstwa wiążącego się z naruszeniem obowiązków określonych w art. 42 ustawy. Innymi słowy, jeżeli do nieautoryzowanej transakcji doszło na skutek ingerencji przestępców w sprzęt lub oprogramowanie klienta, z woli ustawodawcy ryzyko takiego stanu rzeczy ponosi bank, o ile tylko klientowi nie można przypisać umyślności lub rażącego niedbalstwa. Regulacja ta musi być na gruncie postępowania cywilnego oceniona w kontekście art. 6 k.c. Zgodnie bowiem z obowiązującą zasadą ciężaru dowodu (onus probandi) strona winna udowodnić fakty, z których wywodzi korzystne dla siebie skutki prawne. W niniejszej sprawie oznacza to, że pozwany bank zobowiązany był wykazać autoryzowanie transakcji z dnia 30 stycznia 2014 roku przez M. B. (1), czego ostatecznie nie uczynił.

Rażące niedbalstwo (culpa lata) jest kwalifikowaną postacią winy nieumyślnej Oznacza zatem wyższy jej stopień niż w przypadku zwykłego niedbalstwa, leżący już bardzo blisko winy umyślnej (culpa lata dolo aequiparatur). Wykładnia pojęcia rażącego niedbalstwa powinna uwzględniać kwalifikowaną postać braku zwykłej staranności w przewidywaniu skutków. Konieczne jest zatem stwierdzenie, że podmiot, któremu taką postać winy chce się przypisać, zaniedbał takiej czynności zachowującej chronione dobro przed zajściem zdarzenia powodującego szkodę, której niedopełnienie byłoby czymś absolutnie oczywistym w świetle doświadczenia życiowego dostępnego każdemu przeciętnemu uczestnikowi obrotu prawnego i w sposób wprost dla każdego przewidywalny mogło doprowadzić do powstania szkody. Rażące niedbalstwo zachodzi bowiem tylko wtedy, gdy stopień naganności postępowania drastycznie odbiega od modelu właściwego w danych warunkach zachowania się dłużnika (por. wyrok Sądu Najwyższego z dnia 22 kwietnia 2004 roku, II CK 142/03, Lex nr 484721, wyrok Sądu Najwyższego z dnia 25 września 2002 roku, I CKN 969/00, LEX nr 55508, wyrok Sądu Okręgowego w Łodzi z dnia 20 marca 2017 roku, III Ca 1753/16, orzeczenia.lodz.so.gov.pl, wyrok Sądu Okręgowego w Łodzi z dnia 2 maja 2017 roku, III Ca 43/17, III Ca 43/17, orzeczenia.lodz.so.gov.pl, wyrok Sądu Okręgowego w Łodzi z dnia 22 marca 2016 roku, III Ca 24/16, Lex nr 2130586).

Podzielając w pełni powyżej zaprezentowane poglądy judykatury nie sposób mówić o niedbałym zachowaniu powoda, a do tego w stopniu rażącym. M. B. (1) nie udostępnił w sposób całkowicie świadomy (umyślny) swego numeru identyfikacyjnego i hasła, czy też jednorazowego hasła sms, nie przechowywał również tych danych w sposób umożliwiający swobodny dostęp do jego konta osobom niepowołanym.

W dniu 30 stycznia 2014 roku powód zalogował się do internetowego systemu transakcyjnego banku, przy czym żadna z towarzyszących tej czynności okoliczności nie wskazywała, że procedura dostępu jest inna niż zazwyczaj (konieczność podania numeru identyfikacyjnego i hasła, wygląd strony internetowej). W dalszej kolejności M. B. (1) uzupełnił dane na potrzeby przelewu środków tytułem opłaty za gaz, a następnie wpisał uzyskane drogą SMS hasło jednorazowe. Ponownie należy wskazać, że brak jest możliwości wiążącego ustalenia, jaka była treść komunikatu wymuszającego wprowadzenie tych danych, niemniej jednak skoro hasło zostało ostatecznie wpisane i nie budziło większych wątpliwości ze strony powoda to należy przyjąć, że M. B. (1) stosował się do kierowanych względem niego poleceń, aby zrealizować przelew środków pieniężnych tytułem opłaty za gaz. Bezspornym pozostaje fakt, że bez wprowadzenia hasła jednorazowego nie doszłoby do ustanowienia nowego odbiorcy zdefiniowanego (I. K.), jednakże sama wiadomość sms pochodziła od banku, co w zbieżności czasowej z dokonywaną transakcją uwiarygodniało potrzebę wykonanie tej czynności, a jej treść należy ocenić jako mało czytelną dla zwykłego posiadacza rachunku. Brak weryfikacji numerów rachunków (ciąg 26 cyfr) wskazanych w treści wiadomości, a do tego niekompletnych, przy jednoczesnym żądaniu podania hasła jednorazowego przez internetowy system bankowości elektronicznej w warunkach konsolidacji banku i wewnętrznych zmian z nią związanych oraz zamiaru dokonania zwykłej codziennej transakcji (opłata za media) należy ocenić jako zachowanie niedostatecznie uważne ze strony powoda, jednakże niecechujące się rażącym niedbalstwem. Nadto ponownie należy podkreślić, że samo wprowadzenie hasła jednorazowego nie było w tym przypadku równoznaczne z autoryzowaniem nie tylko ustanowienia nowego odbiorcy zdefiniowanego (brak świadomości powoda), lecz przede wszystkim dwóch spornych transakcji środków pieniężnych na rzecz osoby całkowicie nieznanej M. B. (1). Powód swym zachowaniem nie potwierdził w żaden sposób którejkolwiek ze spornych transakcji.

W tak ukształtowanym stanie faktycznym Sąd stwierdził brak podstaw do uznania spornych transakcji za autoryzowane przez powoda, oceny zachowania M. B. (1) jako umyślnego lub cechującego się rażącym niedbalstwem, a także jego przyczynienia się do powstałej szkody w rozumieniu art. 362 k.c. Brak uwagi ze strony powoda w zakresie użycia hasła jednorazowego prowadził jedynie do nieświadomego ustanowienia odbiorcy zdefiniowanego. Gdyby nie jednostronne narzucenie opcji domyślnej w zakresie dalszych operacji na rzecz takiego podmiotu (z określoną kwotą dopiero na tym etapie), transakcje takie wymagałaby autoryzacji. Ostatecznie przebieg wydarzeń był inny, co nie uzasadniania przyjęcia przyczynia się powoda w jakimkolwiek stopniu.

W tym miejscu należy wskazać, że transfer środków pieniężnych nastąpił z konta, które było wykorzystywane sporadycznie, a w praktyce w ogóle nie używane w okresie niemalże 10 lat przed dniem 30 stycznia 2014 roku, a do tego ostatnia znacząca transakcja (32.043,30 złotych) wykonana została w dniu 19 listopada 2004 roku. Uwzględniając przy tym brak uprzedniego używania przez M. B. (1) opcji przelewów S., brak znajomości osoby o danych I. K. oraz modus operandi nieustalonych sprawców nie sposób zanegować tezę, że mężczyzna stał się ofiarą przestępstwa oszustwa komputerowego stypizowanego w art. 287 § 1 kodeksu karnego.

Na marginesie należy stwierdzić, że Sąd nie podziela wniosków biegłego z zakresu informatyki o szczególnej trudności, czy nawet niemożności stworzenia systemu antyfraudowego, który uniemożliwiłby transfer środków w przypadkach jak w realiach niniejszej sprawy, w szczególności w kontekście aktualnego stopnia zaawansowania technologii oraz coraz szerszej wiedzy na temat sposobów działania przestępców. Przyjmując brak możliwości skonstruowania algorytmu antyfraudowego, który sygnalizowałby alert w przypadku transakcji typu S. (pierwszej tego typu z danego rachunku bankowego), operacji dotyczącej znacznej kwoty pieniężnej (wielokrotnie przekraczającej standardowe zachowania klienta banku), a do tego pierwszej tak znaczącej operacji od wielu lat (niemalże 10 lat) należałoby uznać, że tworzenie jakiegokolwiek systemu tego typu jest fikcją i brak jest możliwości przeciwdziałania czynnościom przestępczym nawet w tak oczywistej sytuacji jak w niniejszej sprawie.

W świetle poczynionych rozważań uzasadnionym pozostawało żądanie zwrotu środków pieniężnych z obu transakcji, które nie były autoryzowane przez M. B. (1) wraz z pobraną opłatą za przelew typu S.. Ostateczna wysokość przyznanego świadczenia została jednak pomniejszona na podstawie art. 46 ust. 2 pkt 1 u.u.p. o kwotę równowartości 150 Euro ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania każdej ze spornych transakcji (1 Euro = 4, (...) złotego). W odróżnieniu od treści ust. 3 wskazanego przepisu możliwość ograniczenia wysokości zwrotu nieautoryzowanej transakcji nie jest uzależniona od umyślnego lub rażąco niedbałego zachowania posiadacza rachunku. Tym samym na rzecz powoda przyznano kwotę 53.205,96 złotych (26.127,30 złotych – 635,47 złotych + 28.279,60 złotych – 635,47 złotych + 70 złotych). W pozostałym zakresie powództwo podlegało zaś oddaleniu.

O odsetkach sąd orzekł na podstawie art. 481 k.c. w zw. z art. 46 ust. 1 u.u.p. zgodnie z żądaniem powoda tj. od dnia 14 lutego 2014 roku.

Wysokość odsetek została określona na podstawie art. 481 § 2 k.c. z uwzględnieniem zmiany treści przepisu, jaka nastąpiła z dniem 1 stycznia 2016 roku w związku z wejściem w życie ustawy z dnia 9 października 2015 roku o zmianie ustawy o terminach zapłaty w transakcjach handlowych, ustawy - Kodeks cywilny oraz niektórych innych ustaw (Dz. U. 2015, poz. 1830). Dlatego też w okresie do dnia 31 grudnia 2015 roku przyznano odsetki w wysokości odsetek ustawowych, zaś w okresie od dnia 1 stycznia 2016 roku w wysokości odsetek ustawowych za opóźnienie.

O kosztach procesu sąd orzekł na podstawie art. 100 zd. 2 k.p.c. uznając, że powód uległ co do nieznacznej części swego żądania (53.205,96 złotych / 54.476,90 złotych = 98 %). M. B. (1) poniósł koszty procesu w łącznej kwocie 9.941 złotych (2.724 złotych tytułem opłaty od pozwu – art. 13 ustęp 1 ustawy o kosztach sądowych w sprawach cywilnych, 7.200 złotych tytułem kosztów zastępstwa procesowego - § 2 pkt 6 rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 roku w brzmieniu sprzed nowelizacja z dnia 27 października 2017 roku – Dz.U. 2015, poz. 1804 z późń. zm. oraz 17 złotych tytułem opłaty skarbowej od udzielonego pełnomocnictwa) i w takiej wysokości zostały one przyznane na jego rzecz od pozwanego.

W toku niniejszego postępowania wygenerowane zostały również koszty sądowe, które tymczasowo poniósł Skarb Państwa w kwocie 295,60 złotych tytułem wynagrodzenia biegłego (k.202). Uwzględniając treść art. 113 ustawy o kosztach sądowych w sprawach cywilnych oraz zasadę ponoszenia kosztów procesu w niniejszej sprawie Sąd nakazał pobrać od pozwanego kwotę 295,60 złotych tytułem nieuiszczonych kosztów sądowych.