Sygn. akt: IX C 1760/15

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 6 października 2016r.

Sąd Rejonowy w Opolu IX Wydział Cywilny

w składzie następującym:

Przewodniczący:	SSR Małgorzata Garbowicz
Protokolant:	sekr. sądowy Joanna Romkowska

po rozpoznaniu w dniu 17 marca 2016r., 2 czerwca 2016r., 22 września 2016r. w O.

sprawy ***z powództwa J. K.***

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

o zapłatę

I. zasądza od pozwanej (...) Banku (...) Spółki Akcyjnej w W. na rzecz powoda J. K. kwotę 38.584,82 zł (trzydzieści osiem tysięcy pięćset osiemdziesiąt cztery złote 82/100) z odsetkami ustawowymi za opóźnienie od dnia 3 sierpnia 2015r. do dnia zapłaty, a w pozostałym zakresie żądanie oddala;

II. zasądza od pozwanej (...) Banku (...) Spółki Akcyjnej w W. na rzecz powoda J. K. kwotę 4.203,76 zł (cztery tysiące dwieście trzy złote 76/100) tytułem zwrotu kosztów procesu.

Sygn. akt IX C 1760/15

UZASADNIENIE

W pozwie z dnia 28 września 2015r. J. K. domagał się zasądzenia od pozwanego (...) Banku (...) S.A w W. 39.803,00 zł z odsetkami ustawowymi od dnia 20 maja 2015r. do dnia zapłaty oraz zasądzenia kosztów procesu.

W uzasadnieniu podał, że pozwany prowadzi dla niego rachunek bankowy. Korzystając z usług bankowości elektronicznej, w dniu 20 maja 2015r. powód dokonał na tym rachunku wpłaty należności za wodę. Czynność taka jest autoryzowana sms na telefonie komórkowym powoda. Nazajutrz o godzinie 18 – tej podczas kontroli konta powód stwierdził, że z jego konta przelano na konto w Banku (...) S.A w W. 39.803,00 zł, w dwóch transzach: 19.915,00 zł i 19.888,00 zł. Dokonujący kradzieży miał świadomość, że pobranie kwoty powyżej 20.000,00 zł jest związane z dodatkową kontrolą ze strony Banku. O fakcie tym powód niezwłocznie zawiadomił pozwanego, licząc na natychmiastowe wyrównanie szkody. Szkody nie wyrównano, powodowi polecono by o przestępstwie zawiadomił organy ścigania. Pozwany ostatecznie odmówił zapłaty, twierdząc, że przyczyną kradzieży był zawirusowany komputer powoda.

Pozwany domagał się oddalenia powództwa i zasądzenia kosztów procesu. Przyznał, że strony łączy umowa rachunku bankowego z dnia 10.12.2014r. Zgodnie z § 17 ust. 1 umowy, informacje o zmianach w regulaminach lub taryfie prowizji i opłat powód otrzymuje przez system bankowości elektronicznej. Do umowy rachunku bankowego zastosowanie

miał regulamin rachunków bankowych i kart debetowych dla klientów indywidualnych w (...). Do płatności dokonanych w dniu 19 i 20 maja 2015r. zastosowanie miał regulamin świadczenia usług bankowości elektronicznej w (...) S.A. Zgodnie z § 12 regulaminu świadczenia usług bankowości elektronicznej, klient jest zobowiązany do zachowania w tajemnicy informacji zapewniających bezpieczne korzystanie z usług bankowości elektronicznej oraz nieudostępniania i nieujawniania innym osobom instrumentów uwierzytelniających. Klient zobowiązany jest także do należytego zabezpieczania urządzeń i oprogramowania, którymi posługuje się w celu korzystania z usług bankowości elektronicznej.

Pozwany ustalił, że podczas próby logowania się przez powoda do serwisu internetowego banku, po wprowadzeniu danych do logowania(tj. numeru klienta i hasła dostępu) powód otrzymał fałszywy komunikat z prośbą o podanie kodu z narzędzia autoryzacyjnego. Przy użyciu podanego przez powoda kodu (kod sms), na jego rachunku został zdefiniowany nowy szablon odbiorcy na podstawiony rachunek bankowy. W szablonie tym widniało nazwisko odbiorcy: J. N. i numer rachunku bankowego 90... (...), tytuł płatności:kdn83982110. Kod sms z wyżej podanymi danymi został wysłany na numer telefonu powoda widniejący w umowie rachunku bankowego – (...) w dniu 19 maja 2015r. o godzinie 19.24. Wówczas powód mógł zweryfikować dane z informacji podanych w wiadomości sms. Powód w żaden sposób nie zareagował na tę wiadomość. Nadto powód, wbrew ostrzeżeniom podawanym przez pozwanego i informacjom o obowiązujących zasadach bezpieczeństwa znajdujących się na stronach internetowych banku oraz wbrew postanowieniom regulaminu, udostępnił kod z narzędzia autoryzacyjnego, pomimo że komunikat o podaniu go wystąpił po zalogowaniu się, a więc w sposób odbiegający od zwykłego trybu postępowania. Na stronie internetowej pozwanego, na stronie logowania do (...) znajduje się informacja „Pamiętaj! Logowanie do serwisu (...) nie wymaga podania kodu z karty kodów jednorazowych. Bank również nie poprosi Cię o podanie jednocześnie kilku kodów z karty kodów lub danych karty płatniczej". Powód informacje te zignorował.

Bezsporne było, że przelewy środków z rachunku powoda miały miejsce w dniu 20 maja 2015r. Gdyby powód zareagował niezwłocznie po otrzymaniu danych nowego odbiorcy, do przelewu środków by nie doszło. W związku z utworzeniem szablonu płatności na podstawie podanego przez powoda kodu dostępu, możliwe było zlecenie przelewu środków z rachunku bankowego powoda bez konieczności podawania dodatkowych kodów autoryzacyjnych do każdej transakcji. Akceptacja powoda dotyczyła szablonu płatności z danymi nowego odbiorcy i w związku z tym nie było konieczne akceptowanie przez niego kolejnych transakcji przelewu środków. Pozwany podkreślał, że dochował wszelkiej staranności i przedsięwziął wszelkie możliwe i dostępne środkiw celu zapewnienia bezpieczeństwa przy dokonywaniu transakcji za pomocą (...), natomiast powód nie zachował podstawowych zasad bezpieczeństwa korzystania z serwisu (...) i to z jego wyłącznej winy doszło do przelania środków z jego rachunku bankowego przez osobę trzecią.

Sąd ustalił następujący stan faktyczny:

Na podstawie umowy rachunku oszczędnościowego z dnia 10 grudnia 2014r. roku Bank (...) S.A. w W. prowadził dla powoda J. K. indywidualny rachunek oszczędnościowo - rozliczeniowy pod nazwą konto (...), usług bankowości elektronicznej oraz karty debetowej (bez (...)) nr (...). W umowie nie ustalono dziennego limitu operacji internetowych.

Powód korzystał w pozwanym Banku z usług bankowości elektronicznej. Wykonanie operacji na koncie bankowym wymaga autoryzacji transakcji dokonywanej zależnie od metody autoryzacji wybranej przez klienta: poprzez kod wysyłany sms-em lub kod z papierowej karty dostarczanej użytkownikowi. Powód stosował autoryzację za pomocą kodów wysyłanych sms-ami. Sms-y z kodami generuje bank i dostarcza za pomocą operatora telefonicznego.

Zgodnie z § 17 ust. 1 umowy, informacje o zmianach w regulaminach lub taryfie prowizji i opłat powód otrzymywał przez system bankowości elektronicznej. Do umowy rachunku bankowego zastosowanie miał regulamin rachunków bankowych i kart debetowych dla klientów indywidualnych w (...). Do płatności dokonanych w dniu 19 i 20 maja 2015r. zastosowanie miał regulamin świadczenia usług bankowości elektronicznej w (...) S.A. Zgodnie z § 12 regulaminu świadczenia usług bankowości elektronicznej, klient był zobowiązany do zachowania w tajemnicy

informacji zapewniających bezpieczne korzystanie z usług bankowości elektronicznej oraz nieudostępniania i nieujawniania innym osobom instrumentów uwierzytelniających. Klient zobowiązany był także do należytego zabezpieczania urządzeń i oprogramowania, którymi posługiwał się w celu korzystania z usług bankowości elektronicznej.

Dla uzyskania dostępu do konta drogą elektroniczną, powód musiał zalogować się w serwisie (...), a następnie podać dane identyfikacyjne tj. numer klienta i hasło dostępu. Do autoryzacji transakcji płatniczych konieczne było podanie ponadto żądanego hasła autoryzacyjnego, podanego powodowie przez bank w drodze sms, wysłanego na numer telefonu powoda – (...).

Dowód: umowa z dnia 10.12.2014r., k. 57-62; regulamin, k.63-91, 92-103, 196-219; zeznania świadka D. P., k. 163- 168;

W dniu 19 maja 2015r. powód próbował zalogować się w serwisie internetowym pozwanego Banku po to, aby wykonać przelew należności za wodę na rzecz wspólnoty mieszkaniowej. Po zalogowaniu (tj. po wprowadzeniu numeru klienta i hasła dostępu) do serwisu internetowego Banku, powód otrzymał fałszywy komunikat z prośbą o podanie kodu z narzędzia autoryzacyjnego. Bank wysłał powodowi sms z kodem autoryzacyjnym. Powód wpisał dane kodu z sms na formularzu strony internetowej pozwanego banku. Po dokonaniu przez przestępców internetowych operacji hakerskiej polegającej na założeniu formularzu zdefiniowanego, przy użyciu podanego kodu na rachunku powoda został zdefiniowany przez osoby nieupoważnione nowy szablon płatności na podstawiony (przestępczy) rachunek odbiorcy, który następnie został wykorzystany przez przestępców do realizacji przelewów na jego podstawie. Realizacja powyższych transakcji nastąpiła w wyniku zainfekowania stacji roboczej, z której logował się powód do serwisu (...) złośliwym oprogramowaniem. Wirus zainstalowany na komputerze spowodował, że po zalogowaniu (tj. po wprowadzeniu numeru klienta i hasła dostępu) do serwisu internetowego Banku, powód otrzymał fałszywy komunikat z prośbą o podanie kodu z narzędzia autoryzacyjnego.

Pracownikom pozwanego wiadomo jest, że wirusy „podczepiają się" pod wszystkie strony transakcyjne istniejących banków. Wirus polega na tym, że pojawia się wprowadzająca klientów w błąd informacja o zmianie formatu konta, która ma uzasadnić czynność hakerską, jest to socjotechnika stosowana przez hakerów. Nie ma w 100% skutecznych systemów antywirusowych. Istnieją wersje bezpłatnych programów antywirusowych, które w 80 % udaremnią takie sytuacje.

Dowody: raport wiadomości, k. 104, korespondencja e-mail, k.105, pismo pozwanego, k. 155, pismo, k.156-157,k.158-161, pismo-k.179-186; zeznania świadka D. P., k. 163- 168; zeznania świadka J. G., e-protokół z dnia 22 lutego 2016r. 00:08:37-00:18:38; e- mail z dnia 3 sierpnia 2015r. k.30;

W dniu 19 maja 2015r. o godzinie 19.24 podczas logowania z komputera o adresie (...) został zdefiniowany nowy szablon odbiorcy o następujących danych:

- numer rachunku z: (...);

- numer rachunku na: (...);

- nazwa odbiorcy: J. N.;

- tytuł płatności: (...).

Do potwierdzenia (autoryzacji) dyspozycji zdefiniowania nowego szablonu odbiorcy przelewów posłużył jednorazowy kod sms wysłany na numer telefonu komórkowego powoda 504 201 733. (okoliczność bezsporna).

Dowody: pismo pozwanego, k. 155, pismo, k.156-157,k.158-161, pismo-k.179-186,; zeznania świadka D. P., k. 163- 168; zeznania świadka J. G., e-protokół z dnia 22 lutego 2016r. 00:08:37-00:18:38; e- mail z dnia 3 sierpnia 2015r. k.30;

W dniu 20 maja 2015 r. niezidentyfikowany sprawca dokonał bez wiedzy i zgody powoda operacji na rachunku nr (...), a to:

- przelewu na kwotę 19.915,00 zł między własnymi rachunkami powoda: z rachunku oszczędnościowego o numerze (...) na jego rachunek (...) nr. (...) w dniu 20 maja 2015r., podczas logowania z komputera o adresie (...). Transakcja została zrealizowana w dniu 20 maja 2015r. o godzinie 9.12; do realizacji przelewu pomiędzy własnymi rachunkami nie jest wymagany kod autoryzacyjny;

- w dniu 20 maja 2015r. podczas tego samego logowania z komputera o adresie (...)został zlecony przelew na podstawie utworzonego wcześniej szablonu odbiorcy, na kwotę 19.915,00 zł z rachunku klienta nr (...) (A.) na rachunek nr (...). Transakcja została zrealizowana w dniu 20 maja 2015r. o godzinie 9.13; do realizacji przelewu na podstawie wcześniej zdefiniowanego szablonu odbiorcy nie jest wymagany kod autoryzacyjny;

- w dniu 20 maja 2015r. podczas logowania z komputera o adresie (...). został zlecony przelew na kwotę 5.000,00 zł między własnymi rachunkami klienta: z rachunku (...) o numerze (...) na jego rachunek (...) nr. (...). Transakcja została zrealizowana w dniu 20 maja 2015r. o godzinie 11.58; do realizacji przelewu pomiędzy własnymi rachunkami nie jest wymagany kod autoryzacyjny;

- w dniu 20 maja 2015r. podczas tego samego logowania z komputera o adresie (...) został zrealizowany przelew na podstawie utworzonego wcześniej szablonu odbiorcy, na kwotę 19.888,00 zł z rachunku klienta nr (...)(A.) na rachunek nr (...). Transakcja została zrealizowana w dniu 20 maja 2015r. o godzinie 11.59; do realizacji przelewu na podstawie wcześniej zdefiniowanego szablonu odbiorcy nie jest wymagany kod autoryzacyjny.

Dowody: zestawienie operacji na rachunku bankowym. 151-154, pismo pozwanego, k. 105,155, pismo, k.156-157,k.158-161, pismo-k.179-186;

Pozwany Bank ustalił, że wyżej opisane transakcje zostały zlecone po poprawnym zalogowaniu w serwisie (...) numerem oraz hasłem dostępu powoda. Realizacja powyższych transakcji nastąpiła w wyniku zainfekowania stacji roboczej, z której logował się powód do serwisu i (...) złośliwym oprogramowaniem. Wirus zainstalowany na komputerze spowodował, że po zalogowaniu (tj. po wprowadzeniu numeru klienta i hasła dostępu) do serwisu internetowego Banku, powód otrzymał fałszywy komunikat z prośbą o podanie kodu z narzędzia autoryzacyjnego. Przy użyciu podanego kodu na rachunku powoda został zdefiniowany przez osoby nieupoważnione nowy szablon płatności na podstawiony(przestępczy) rachunek odbiorcy, który następnie został wykorzystany przez przestępców do realizacji przelewów na jego podstawie.

Dowody: e- mail z dnia 3 sierpnia 2015r. k.30;

Pozwany Bank ustalił także, że sposób kradzieży pieniędzy z konta powoda był podobny do kradzieży środków z kont innych klientów Banku, które miały miejsce pod koniec maja 2015r. Kradzieży tych dokonano za pomocą oprogramowania malware emotet, które działa pod N. (...), wyświetla użytkownikowi komunikat „zmiana formatu konta", pyta o kod autoryzacyjny, nieświadomy klient dodaje nową płatność, która jest ukrywana przed właścicielem konta. Czynności wykonywane są w następującej kolejności:

- po zalogowaniu wysyła na serwer: login, hasło, dostępne środki;

- klika odbiorcy – nowy odbiorca krajowy;

- modyfikuje popup: ukrywa pola oryginalnego formularza i dodaje swój komunikat (wizualizacja w kom 1 zmiana formatu konta.png.);

- po kliknięciu „dalej" wyświetla pytanie o kod autoryzacyjny (wizualizacja w kom. 1 kod.png.);

- wyświetlony jest komunikat z potwierdzeniem, gdy nowa płatność została dodana(wizualizacja w kom. 1 potwierdzenie. P..);

- dodana fraudowa płatność jest ukrywana w interfejsie;

- przestępcy mają również możliwość wyświetlenia komunikatu o niedostępności serisu (wizualizacja w blokowanie.png.);

- nie ma w skrypcie dokumentów, które wykonują transakcje automatycznie, dlatego najprawdopodobniej czyszczenie konta (wykorzystanie płatności) odbywa się z innej sesji.

Dowód: pismo pozwanego k.156-157;

W dniu 19 maja 2015r. powód logował się na stronę banku ze stacjonarnego komputera, na którym zainstalowany był legalny system operacyjny oraz oprogramowanie antywirusowe McAfee dostarczone przez informatyka M. K. i cyklicznie przez niego sprawdzane. Powód czytał komunikaty dotyczące bezpieczeństwa pojawiające się na stronie Banku. Powód nie podawał nikomu loginu i hasła do swojego konta w pozwanym Banku.

zeznanie świadka M. K. e-protokół z dnia 22 września 2016r., 00: 03: 34-00: 35:00; przesłuchanie powoda, e-protokół z dnia 22 września 2016r., 00:13:34-00:37:00;

W dniu 21 maja 2015 r. powód zalogował się na swoje konto i stwierdził wykonanie przelewów, których nie zlecał i nie autoryzował. Powód nie zna osoby, na której konto zostały wykonane przelewy z jego konta. W dniu 21 maja 2015 r. powód poprzez infolinię złożył pozwanemu reklamację dotyczącą nieautoryzowanych przelewów. Reklamację w tym przedmiocie złożył również na piśmie w dniu 22 maja 2015r. W dniu 25 maja 2015r. powód złożył zawiadomienie o popełnieniu przestępstwa w Prokuraturze Rejonowej w Opolu.

Po złożeniu reklamacji z powodem skontaktował się pracownik pozwanego banku, który poinformował go, że wyżej opisana sytuacja jest przedmiotem analizy.

W dniu 3 sierpnia 2015r. pozwany poinformował powoda, że ustalił, iż wyżej opisane transakcje zostały zlecone po poprawnym zalogowaniu w serwisie (...) numerem oraz hasłem dostępu powoda. Realizacja powyższych transakcji nastąpiła w wyniku zainfekowania stacji roboczej, z której logował się powód do serwisu i (...) złośliwym oprogramowaniem. Wirus zainstalowany na komputerze spowodował, że po zalogowaniu (tj. po wprowadzeniu numeru klienta i hasła dostępu) do serwisu internetowego Banku, powód otrzymał fałszywy komunikat z prośbą o podanie kodu z narzędzia autoryzacyjnego. Przy użyciu podanego kodu na rachunku powoda został zdefiniowany przez osoby nieupoważnione nowy szablon płatności na podstawiony(przestępczy) rachunek odbiorcy, który następnie został wykorzystany przez przestępców do realizacji przelewów na jego podstawie.

Dowody: pismo powoda, k.22, pismo powoda, k.23, k.30, pismo pozwanego, k. 24, 25, e- mail z dnia 3 sierpnia 2015r. k.30;

Sąd zważył, co następuje:

Powództwo zasługiwało na uwzględnienie w przeważającej części.

Zgodnie z art. 725 kc 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.

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 (SN w wyr. z 14.4.2003 I CKN 308/61)

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. Podstawę prawną roszczenia powoda stanowią przepisy ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (t. jedn. Dz. U. z 2014 r., poz. 873 ze zmianami) określającej między innymi prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych, a także zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych (art. 1 pkt 2 ustawy).

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

W ocenie Sądu pozwany Bank nie wywiązywał się z obowiązku zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. W szczególności nie zapewnił, by indywidualne zabezpieczenia instrumentu płatniczego nie były dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu.

Powód natomiast swoim obowiązkom wymienionym w art. 42 ust. 2 ustawy uchybił, udostępniając instrument płatniczy osobom nieuprawnionym przez wpisanie w dniu 19 maja 2015 r. stronie internetowej Banku kodu autoryzacyjnego przesłanego mu w drodze sms, nie upewniwszy się czy dane podane w wiadomości sms odpowiadają danym tego podmiotu, któremu zamierzał przekazać środki ze swojego konta. Udostępnienie przez powoda tych danych osobom nieuprawnionym o nieustalonej tożsamości umożliwiło tym osobom wykonanie wyżej opisanych przelewów. Aczkolwiek czynności te z punktu widzenia systemu informatycznego Banku były przeprowadzone poprawnie, przy wykorzystaniu właściwych narzędzi autoryzacyjnych, to jednak transakcji płatniczych wykonanych z konta powoda w dniu 20 maja 2015r. nie można uznać, za transakcje autoryzowane. Zgodnie z art. 40 ust. 1 powołanej wyżej ustawy transakcję uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji w sposób przewidziany w umowie między płatnikiem a jego dostawcą. W świetle poczynionych w sprawie ustaleń nie ulega wątpliwości, że powód takiej zgody nie wyraził. Świadczy o tym również fakt, że niezwłocznie powiadomił pozwanego oraz Prokuraturę Rejonową w Opolu, stosownie do obowiązków wynikających z art. 44 ust. 1 ustawy, celem wyjaśnienia przyczyn utraty z konta posiadanych przez niego pieniędzy.

W myśl art. 45 ustawy o usługach płatniczych, ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana.

W okolicznościach niniejszej sprawy nie można powodowi przypisać zgody ani woli podjęcia czynności zmierzających do przeprowadzenia opisanych wyżej transakcji płatniczych przy użyciu posiadanych przez niego instrumentów płatniczych, które to okoliczności świadczyłyby o autoryzowaniu przez niego transakcji. Z materiału dowodowego nie wynika, aby powód umyślnie doprowadził do nieautoryzowanych transakcji płatniczych, choćby z tej przyczyny, że zostały one przeprowadzone bez jego wiedzy.

Zdaniem Sądu powodowi nie można przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa w naruszeniu obowiązków, wynikających z art. 42 ustawy. Aczkolwiek powód udostępnił osobom nieuprawnionym kod z narzędzia autoryzacyjnego, czego nie powinien czynić, to jednak nie nastąpiło to w okolicznościach świadczących o rażącym niedbalstwie z jego strony. W sprawie ustalono, że powód wpisał dane kodu autoryzacyjnego, po poprawnym zalogowaniu się w serwisie (...), na stronie internetowej tego serwisu. Jak wynika ze zgromadzonego w sprawie materiału dowodowego, w szczególności z zeznań świadka D. P., do zainfekowania komputera użytkownika usług bankowości elektronicznej może dojść w podstępny sposób. Z materiału dowodowego nie wynika, aby w okresie poprzedzającym kwestionowane transakcje pozwany Bank wysyłał komunikaty do klientów o sposobach kradzieży pieniędzy z konta za pomocą oprogramowania malware emotet. Wszystkie przelewy, których dotyczy sprawa nie były weryfikowane telefonicznie przez pozwanego. Z przeprowadzonych dowodów wynika, że zostały one wykonane w sposób wyglądający na poprawny, miała miejsce poprawna weryfikacja klienta, operacja polegająca na stworzeniu przelewu zdefiniowanego została potwierdzona kodem jednorazowym z sms – a wysłanego na zarejestrowany numer telefonu powoda. Kod ten został poprawnie użyty. Zarazem z materiału dowodowego nie wynika, aby powód przekazywał pocztą elektroniczną informacje dotyczące jego kont w pozwanym Banku.

Sąd ustalił, że w dniu 19 maja 2015r. powód korzystał z komputera w swoim domu. Powód nikomu nie udostępnił loginu i hasła dostępu do konta. Podkreślić należy, iż powód starał się zapobiec zainfekowaniu komputera wirusem, w tym celu zainstalował legalne oprogramowanie oraz jeden z najskuteczniejszych systemów antywirusowych. Z materiału dowodowego wynika, że właśnie na stronie internetowej pozwanego Banku, a nie w innym miejscu i okolicznościach, zażądano od powoda podania konkretnego hasła z przesłanego mu przez Bank sms-a. Po poprawnym zalogowaniu się w serwisie (...), należącym do pozwanego, powodowi wyświetliła się witryna, o treści i wyglądzie dziś już niemożliwym do odtworzenia, na której żądano podania kodu autoryzacyjnego. Żądanie to, mogło przedstawiać się wiarygodnie, skoro powód był przeświadczony, że jeżeli korzysta ze strony internetowej pozwanego Banku, to komunikat może pochodzić wyłącznie od pozwanego. Bank nie ostrzegał w dacie zdarzenia swoich klientów przed tego rodzaju komunikatami, nie informował, iż skorzystanie z nich może nieść za sobą negatywne skutki. Jak zeznawał świadek D. P. „...Wirusem, który dostał się na komputer powoda hakerzy przejęli hasło i login powoda do wykonywania przelewów. Na pewno powodowi pojawiło się okno z tym rachunkiem z SMS-a by go wprowadzić w błąd. Były to socjotechniki stosowane przez hakerów." Ponadto na podstawie dokumentów przedłożonych przez pozwanego Sąd ustalił, że w maju 2015r. klientów pozwanego Banku „atakował wirus" malware. Skoro właśnie na stronie Banku, a nie w innym miejscu i okolicznościach, zażądano od powoda podania konkretnego hasła z przesłanego mu przez Bank sms-a, to w ocenie Sądu, powyższa okoliczności, nie pozwala na przypisanie powodowi rażącego niedbalstwa. Zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych 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.

Jeżeli nieautoryzowana transakcja jest skutkiem nieuprawnionego użycia instrumentu płatniczego w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2, płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji. Ponieważ powód dopuścił się, obiektywnie rzecz ujmując, naruszenia jednego ze swoich obowiązków ciążących na nim z mocy art. 42 ust. 2 ustawy o usługach płatniczych, winien ponieść odpowiedzialność za nieautoryzowane przelewy z jego konta do wysokości wyżej wskazanej. Ustawodawca zadecydował o takim właśnie rozkładzie ryzyka nieautoryzowanych transakcji między płatnikiem i dostawcą usługi płatniczej w razie naruszenia przez płatnika jednego z jego obowiązków, choćby w sposób niezawiniony (nawet w razie posłużenia się przez osobę nieuprawnioną skradzionym płatnikowi instrumentem płatniczym - art. 46 ust. 2 pkt 1).

Mając na uwadze powyższe Sąd zasądził na rzecz powoda kwotę 38.584.82 zł, pomniejszając żądaną przez powoda kwotę 39.803 zł zgodnie z dyspozycją art. 46 ust. 2 ustawy w następujący sposób:

– 19.915 zł przelane z konta w dniu 20 maja 2015 r. o godz. 9:13, o 609,09 zł, odpowiadające równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego euro ogłaszanego przez NBP i obowiązującego w dniu wykonania tej transakcji (1 euro = 4,0606 zł),

- 19.888 zł przelane z konta w dniu 20 maja 2015 r. o godz. 11:59, o 609,09 zł, odpowiadające równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego euro ogłaszanego przez NBP i obowiązującego w dniu wykonania tej transakcji.

W pozostałym zakresie powództwo podlegało oddaleniu, jako nieuzasadnione.

Ponieważ pozwany dopuścił się opóźnienia w zwrocie zasądzonej wyrokiem kwoty, powodowi należały się odsetki w wysokości ustawowej zgodnie z art. 481 § 1 i 2 k.c. od dnia 3 sierpnia 2015 r. (do dnia zapłaty). W tej dacie Bank wystosował do powoda odpowiedź na reklamację (pismo powoda na k.30), informując o poczynionych ustaleniach dotyczących transakcji z dnia 20 maja 2015r. Wówczas pozwany niewątpliwie posiadał już wiedzę o okolicznościach niezbędnych dla ustalenia własnej odpowiedzialności. Odmawiając powodowi zwrotu środków pieniężnych, popadł z tą chwilą w opóźnienie. Żądanie odsetek w dalej idącym zakresie podlegało oddaleniu.

Odnosząc się do zarzutu pozwanego, że powód, wbrew postanowieniom regulaminu, udostępnił kod z narzędzia autoryzacyjnego, wyjaśnić należy, że zasadniczo powoda nie wiążą te postanowienia regulaminu, które są dla niego mniej korzystne niż przepisy ustawy o usługach płatniczych. Zgodnie bowiem z treścią art. 8 ust. 1 i 2 Ustawy o usługach płatniczych „postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego nie mogą być mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy, chyba że ustawa stanowi inaczej. Postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy są nieważne zamiast nich stosuje się odpowiednie przepisy ustawy". Wprowadzenie przez pozwany bank mniej korzystnych dla klienta regulacji niż ustawowe stanowi naruszenie art. 8 ust. 1 Ustawy o usługach płatniczych, prowadząc do nieważności regulaminowych postanowień, na które powołuje się pozwany.

O kosztach postępowania Sąd Rejonowy orzekł w oparciu o art. 100 k.p.c. zgodnie z zasadą stosunkowego ich rozdzielenia przyjmując, iż powód wygrał proces w 97%. Suma wszystkich kosztów poniesionych przez obie strony 6.808,00 zł. Strony poniosły następujące koszty: powódka - opłata od pozwu 1.991,00 zł, wynagrodzenie radcy prawnego powoda 2.400,00 zł, pozwany - wynagrodzenie radcy prawnego 2.400,00 zł i opłata skarbowa od pełnomocnictwa – 17,00 zł; Powód wygrał sprawę w 97%, powinien zatem partycypować w części przegranej, tj. w 3%, a strona pozwana w 97% kosztów. 53% z łącznej kwoty 6.817,00 zł daje kwotę 3.613,01 zł. Różnica pomiędzy kosztami, które powód powinien zapłacić ze względu na wynik procesu a tymi, które dotąd poniósł wynosi 4.203,76 zł i taką kwotę zasądzono od pozwanego na rzecz powoda (6.808,00 x3%=204,24; 2.400,00 + 17+1991=4.408; 4.408-204,24=4.203,76).

Mając powyższe na względzie orzeczono jak w wyroku.