Sygn. akt VI ACa 217/17

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 24 maja 2018 r.

Sąd Apelacyjny w Warszawie VI Wydział Cywilny w składzie:

Przewodniczący - Sędzia SA – Agata Zając

Sędzia SA – Małgorzata Borkowska (spr.)

Sędzia SA – Teresa Mróz

Protokolant: Małgorzata Samuła

po rozpoznaniu w dniu 10 maja 2018 r. w Warszawie

na rozprawie

sprawy z powództwa S. C.

przeciwko Bankowi (...) S.A. w W.

o zapłatę

na skutek apelacji pozwanego

od wyroku Sądu Okręgowego w Warszawie

z dnia 15 grudnia 2016 r., sygn. akt XXV C 14/16 r.

I. oddala apelację;

II. zasądza od Banku (...) S.A. w W. na rzecz S. C. 4050 zł (cztery tysiące pięćdziesiąt złotych) tytułem zwrotu kosztów postępowania apelacyjnego.

Sygn. akt VI ACa 217/17

UZASADNIENIE

S. C. pozwem z dnia 1 kwietnia 2015r. przeciwko Bankowi (...) S.A. z siedzibą w W. (obecnie: Bank (...) S.A. z siedzibą w W.), sprecyzowanym pismem z dnia 24 listopada 2016r. wniósł o: zasądzenie od pozwanego na rzecz powoda kwoty 85.000 zł wraz z odsetkami ustawowymi od dnia 17 lutego 2014 r. do 31 grudnia 2015 r. oraz ustawowymi odsetkami za opóźnienie od 1 stycznia 2016 r. do dnia zapłaty, ewentualnie w wypadku, uznania przez Sąd, iż brak jest przestanek do zasądzenie odsetek od dnia 17 lutego 2014 r. wniósł o zasądzenie odsetek ustawowych od dnia wniesienia pozwu oraz zasądzenie zwrotu kosztów postępowania w tym kosztów zastępstwa prawnego wg norm prawem przepisanych.

W uzasadnieniu wskazał, że materialną podstawą jego żądania jest art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. nr 199, poz. 1175 ze zm.), gdyż doszło do nieautoryzowanej transakcji płatniczej, przez co w drodze działań przestępczych hakerzy wyprowadzili z jego rachunku bankowego środki pieniężne w wysokości 85.000 zł. Wskazał, że sprawcy przejęli kontrolę nad komputerem powoda, ustanowili na jego koncie użytkownika zaufanego poprzez wysłanie na jego telefon w formie wiadomości sms, komunikatu imitującego wiadomość od banku. Sms był w szacie graficznej łudząco podobny do wiadomości przesyłanych przez bank, w konsekwencji użytkownik

nie był w stanie zorientować się, że komunikat nie jest autentyczny. Wprowadzony w błąd, zdecydował o akceptacji zmiany formatu konta, jednak sms okazał się zwykłym wyłudzeniem kodu autoryzacyjnego, co doprowadziło w konsekwencji do ustanowienia przez hakerów użytkownika zaufanego o nazwie (...). Po ustanowieniu użytkownika zaufanego, sprawcy dokonali szeregu transakcji, które nie wymagały już autoryzacji. Były one przeprowadzane bez świadomości i wiedzy powoda, który o ich zaistnieniu dowiedział się dopiero po zalogowaniu się na konto w dniu 17 stycznia 2014 r. Powód podkreślił, że dochował należytej staranności w korzystaniu z serwisu transakcyjnego banku. Przede wszystkim był wyłącznym użytkownikiem swojego loginu i hasła do internetowego konta - nie udostępniał ich osobom postronnym. Dotyczy to także telefonu oraz komputera. Nadto na komputerze zainstalowany był program antywirusowy (...). O nieautoryzowanych transakcjach zawiadomił niezwłocznie pozwany bank. Nadmienił też, że w dniu 9 grudnia 2014 r. Sąd Rejonowy w Zawierciu (...) Wydział (...) w sprawie o sygn. II K 1053/14 wydał (prawomocny) wyrok zaoczny, na mocy którego uznał oskarżonego A. N. (1) za winnego popełnienia zarzucanego mu czynu polegającego na złamaniu zabezpieczeń elektronicznych do konta bankowego (...) S.A. o nr (...) prowadzonego dla pokrzywdzonego S. C., a następnie dodaniu swojego konta jako zidentyfikowany odbiorca, skąd po zerwaniu lokat związanych z kontem pokrzywdzonego przelał pieniądze na swoje konto zabierając w celu przewłaszczenia pieniądze w kwocie 85.000 zł na szkodę S. C., tj. przestępstwa z art. 279 § 1 kk i art. 267 § 1 kk w zw. z art. 11 § 2 kk. Już tylko na tej podstawie można stwierdzić – zdaniem powoda -, że zlikwidowanie lokat oraz pobranie środków z konta bankowego powoda nastąpiło bez jego wiedzy, a co najważniejsze nie było po jego stronie zamiaru, bądź chęci dokonania takich przesunięć majątkowych.

Powołując się na ustawę o usługach płatniczych, powód wskazał także, że dla zwolnienia się z ponoszenia odpowiedzialności za nieautoryzowane transakcje, bank jest obowiązany wykazać przesłanki z art. 45 ust. 2 oraz art. 46 ust. 3, które w niniejszej sprawie nie zaistniały. W niniejszej sprawie nie można bowiem wskazywać na umyślność w zakresie dokonanych transakcji po stronie powoda. Niemożliwe jest także określenie podejmowanych przez niego zachowań, jako rażącego niedbalstwa.

W odpowiedzi na pozew pozwany wniósł o oddalenie powództwa w całości oraz zasądzenie od powoda na rzecz pozwanego kosztów procesu oraz kosztów zastępstwa procesowego według norm przepisanych.

W uzasadnieniu podał, że w dniu 14 stycznia 2014 r. po dokonaniu prawidłowego logowania do systemu (...) dodano zdefiniowanego zaufanego kontrahenta o nazwie (...) o nr rachunku (...) przy czym operacja ta została zatwierdzona prawidłowym kodem sms, wysłanym na numer wskazany przez powoda. Po dokonaniu kolejnego prawidłowego logowania do systemu (...) w tym dniu zerwano trzy lokaty na łączną kwotę 70.000 złotych oraz dokonano trzech przelewów z rachunku powoda na rzecz zdefiniowanego uprzednio kontrahenta pod nazwą (...) odpowiednio na kwotę 15.000 złotych oraz dwa przelewy na kwoty po 35.000 złotych. Każdego logowania dokonano przy użyciu unikalnego loginu powoda i unikalnego hasła wybranego przez powoda. W związku z tym – w ocenie pozwanego - zostały one wykonane zgodnie z wymogami ustalonymi przez strony. Bank nie odnotował w tym czasie żadnych awarii, ani innych defektów systemu bankowości elektronicznej, a w konsekwencji zlecenie zostało wykonane zgodnie z dyspozycją.

Pozwany podniósł, że w wyroku z dnia 9 grudnia 2014 r. wydanym w sprawie o sygn. akt II K 1053/14, Sąd Rejonowy w Zawierciu (...) Wydział (...) zobowiązał oskarżonego A. N. (1) do naprawienia szkody poprzez zapłatę na rzecz pokrzywdzonego S. C. kwoty 85.000 zł w terminie jednego miesiąca od uprawomocnienia się wyroku. Powód dysponuje już prawomocnym wyrokiem karnym obejmującym całość szkody wyrządzonej powodowi z tytułu kwestionowanych przez niego transakcji, tj. 85.000 złotych, niniejsze powództwo powinno być oddalone, gdyż kwota zasądzona wyrokiem karnym pokrywa w całości roszczenie główne powoda dochodzone od pozwanego niniejszym pozwem. Uwzględnienie powództwa, prowadziłoby natomiast do powstania dwóch tytułów egzekucyjnych obejmujących to samo roszczenie, a po nadaniu klauzuli wykonalności - dwóch tytułów wykonawczych, co mogłoby doprowadzić do dwukrotnego pokrycia szkody, poprzez ściągnięcie od dwóch różnych dłużników, z dwóch tytułów wykonawczych, tej samej kwoty.

Pozwany wskazał także, że wielokrotnie informował powoda o zasadach bezpieczeństwa dotyczących korzystania z instrumentu płatniczego.

Wyrokiem z dnia 15 grudnia 2016r. Sąd Okręgowy w Warszawie:

zasądził od Banku (...) S.A. na rzecz S. C. kwotę 85.000 złotych wraz ustawowymi odsetkami od tej kwoty od dnia 1 kwietnia 2015 roku do dnia 31 grudnia 2015 roku i z odsetkami ustawowymi za opóźnienie od tej kwoty od dnia 1 stycznia 2016 roku do dnia zapłaty (pkt1);

w pozostałym zakresie powództwo oddalił (pkt 2) oraz orzekł o kosztach procesu (pkt3).

Powyższy wyrok został wydany w oparciu o następujące ustalenia faktyczne i rozważania prawne.

W dniu 20 lipca 2010 r. powód S. C. zawarł z oddziałem pozwanego (wówczas działającym pod nazwą: Bank (...) S.A. z siedzibą w W.) umowę o prowadzenie rachunków bankowych, o kartę płatniczą wydawaną do konta osobistego oraz o korzystanie z systemów bankowości telefonicznej i internetowej. Na podstawie ww. umowy, bank otworzył i prowadził konto osobiste powoda o nr rachunku (...), a poprzez dostęp do konta klient miał możliwość skorzystania z innych usług banku, w tym otwarcia lokat terminowych.

Powód korzystał w pozwanym Banku z usług bankowości elektronicznej.

Aby uzyskać dostęp do konta za pośrednictwem Internetu, klient pozwanego podaje dane identyfikacyjne, tj. pierwszą literę imienia i nazwiska oraz hasło. Do autoryzacji transakcji płatniczych konieczne jest natomiast podanie ponadto żądanego jednorazowego hasła (numerów identyfikacyjnych) przesyłanego drogą sms. Hasła jednorazowe nie są wykorzystywane w pozwanym Banku do identyfikacji klientów na etapie logowania, a jedynie do autoryzacji transakcji. Jedną z dostępnych usług w serwisie transakcyjnym Banku, jest możliwość dodania do konta użytkownika, tzw. zdefiniowanego zaufanego kontrahenta – wykonanie przelewu na rzecz takiego odbiorcy (kontrahenta) nie wymaga potwierdzenia transakcji kodem sms. Przy każdym innym odbiorcy (tzw. „niezaufanym") transakcja przelewowa musi być potwierdzona specjalnym jednorazowym kodem sms, aby mogła dojść do skutku..

Pozwany Bank zamieszcza na swoich stronach internetowych ostrzeżenia o zagrożeniach w systemach bankowości internetowej, w tym dotyczących wirusów i niebezpieczeństw związanych z ich instalowaniem. Ponadto informuje klientów, że nigdy nie wymaga instalowania na komputerach ani telefonach komórkowych żadnego dodatkowego oprogramowania lub certyfikatów. Ostrzeżenia są aktualizowane, gdy pojawia się bądź zmienia zagrożenie. Komunikaty wyświetlane są na stronie logowania lub wysyłane bezpośrednio do klienta i prezentowane już po zalogowaniu w jego skrzynce odbiorczej.

W dniu 14 stycznia 2014 r., powód logował się do internetowego systemu transakcyjnego Banku – na ten dzień posiadał u pozwanego trzy lokaty terminowe na kwoty odpowiednio: 10.000 zł, 50.000 zł oraz 10.000 zł, a nadto niewykorzystany limit kredytu odnawialnego w wysokości 10.000 zł oraz wolne środki na rachunku rozliczeniowym w wysokości 5.275 zł. W tym dniu miał problemy z poprawnym wylogowaniem się z systemu transakcyjnego Banku, gdyż strona internetowa wykazywała oznaki „zawieszenia się".

Powód logował się do serwisu transakcyjnego (...) tylko z jednego prywatnego laptopa. Sprzęt komputerowy miał zainstalowane aktualne oryginalne oprogramowanie antywirusowe firmy (...). Powód nigdy nikomu osobiście nie udostępniał hasła, telefonu ani laptopa, z których korzystał logując się do serwisu internetowego banku. Telefon komórkowy dedykowany do przesyłania kodów sms zawsze nosił przy sobie.

Podczas jednego z logowań, na stronie logowania wyświetlił się komunikat z informacją o zmianie formatu konta i prośbą o potwierdzenie zmiany kodem sms – jednocześnie otrzymał wiadomość sms z kodem autoryzującym, który przepisał na wyświetloną stronę internetową wyglądającą, jak strona logowania do serwisu transakcyjnego pozwanego Banku. Po tym, nie miał problemu by ponownie zalogować się do swojego konta internetowego.

Po zalogowaniu się do systemu bankowości internetowej (...) w dniu 17 stycznia 2014 r. powód stwierdził, że zlikwidowane zostały wszystkie jego lokaty bankowe, a z rachunku przelano środki w łącznej kwocie 85.000 zł na nieznane powodowi konto o nr (...).

W tym samym dniu, niezwłocznie po stwierdzeniu tego faktu powód poinformował telefonicznie Bank o zaistniałej sytuacji, a także udał się osobiście do oddziału Banku w Z., gdzie w obecności pracownika pozwanej - M. S. stwierdził, że wśród zdefiniowanych zaufanych kontrahentów uprawnionych do otrzymywania przelewów z konta powoda bez konieczności potwierdzania transakcji przelewowych kodem sms, znajduje się nieznany powodowi odbiorca (kontrahent) o nazwie „(...)". Powód nigdy nie dodawał wskazanego kontrahenta do listy odbiorców zaufanych, ani nie otrzymał z Banku informacji sms weryfikującej osobnym kodem wykonanie takiej czynności.

W dniu 17 stycznia 2014 r. powód powiadomił o zaistniałym zdarzeniu organy ścigania. W toku prowadzonego dochodzenia, ustalono adresy IP, z których logowano się w dniu 14 stycznia 2014 r. do konta powoda. Ustalono także, że sprawca, używał prawdopodobnie programu maskującego IP działającego na zasadzie wskazywania nieprawdziwego adresu IP komputera, którym się posługiwał.

Rachunek nr (...), na który przelano pieniądze wyprowadzone z konta powoda, był prowadzony na rzecz A. N. (1) – pieniądze z tego rachunku zostały ostatecznie wypłacone w Danii w wielu transzach po 10 000 koron duńskich.

W dniu 9 grudnia 2014 r. Sąd Rejonowy w Zawierciu (...) Wydział (...) w sprawie o sygn. akt II K 1053/14 wydał (prawomocny obecnie) wyrok zaoczny, na mocy którego uznał oskarżonego A. N. (1) za winnego popełnienia zarzucanego mu czynu polegającego na złamaniu zabezpieczeń elektronicznych do konta bankowego (...) S.A. o nr (...) prowadzonego dla pokrzywdzonego S. C., a następnie dodaniu swojego konta jako zidentyfikowany odbiorca, skąd po zerwaniu lokat związanych z kontem pokrzywdzonego przelał pieniądze na swoje konto zabierając w celu przewłaszczenia pieniądze w kwocie 85.000 zł na szkodę S. C., tj. przestępstwa z art. 279 § 1 kk i art. 267 § 1 kk w zw. z art. 11 § 2 kk. Ponadto, na podstawie art. 72 § 2 kk w wyroku zobowiązano oskarżonego do naprawienia szkody poprzez zapłatę na rzecz pokrzywdzonego S. C. kwoty 85.000 złotych w terminie jednego miesiąca od uprawomocnienia się wyroku.

Przed zdarzeniami z dnia 14 stycznia 2014 r. Bank nie informował swoich klientów o zagrożeniach związanych z komunikatem o zmianie formatu konta, tj. o zagrożeniu takimi sposobami działania hakerów, jakie zastosowali oni w przypadku powoda, komunikat na stronie Banku, dotyczący wskazanego zamieszczony dopiero dnia 3 lutego 2014 r.

Sąd uznał, że powództwo zasługiwało na uwzględnienie, powołał się na regulację zawartą w art. 725 k.c. dot. umowy rachunku bankowego. Z mocy wskazanego przepisu 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.

Sąd odwołał się do poglądu, że 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 14 kwietnia 2003 r. sygn. 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 więc bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową.

Równoległą podstawą odpowiedzialności banku jest ustawa o usługach płatniczych z dnia 19 sierpnia 2011 r. (t. jedn. Dz. U. z 2014 r., poz. 873 ze zm.), w której znajduje oparcie roszczenie pozwu. Przywołana ustawa określa, 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). Bank krajowy jest dostawcą usług płatniczych w rozumieniu ustawy (art. 4 ust. 1 i ust. 2 pkt 1). Przez usługi płatnicze rozumie się działalność polegającą 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 (art. 3 pkt 2 lit. c). 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). Zlecenie płatnicze, zgodnie z art. 2 pkt 10 ustawy, płatnik składa 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).

Strony niniejszego postępowania umówiły się, że zgoda na wykonanie transakcji płatniczych za pośrednictwem usług bankowości elektronicznej świadczonych przez pozwany Bank będzie przez powoda udzielana – po zalogowaniu się do konta za pomocą danych identyfikacyjnych składających się z loginu i hasła oraz przez podanie autoryzacyjnego kodu sms i powtórzenie wyświetlonego na stronie zestawu znaków.

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).

Jak wynika z poczynionych ustaleń, pozwany Bank wywiązywał się z obowiązku zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są 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 przynajmniej raz w dniu 14 stycznia 2014 r. kodu autoryzacyjnego podanego w treści wiadomości sms, na podstawionej stronie internetowej, choć w sposób niezamierzony i nieświadomy.

Powód przyznał, że wpisał kod autoryzacyjny na stronie internetowej, która była łudząco podobna do strony pozwanego Banku. Udostępnienie przez powoda za pośrednictwem podstawionej witryny internetowej swoich danych identyfikacyjnych oraz kodu autoryzacyjnego sms będącego w jego posiadaniu osobom nieuprawnionym, umożliwiło tym osobom dodanie do konta powoda tzw. zdefiniowanego odbiorcy zaufanego i wykonanie przelewów na łączną kwotę 85.000 zł.

Czynności te z punktu widzenia systemu informatycznego Banku były przeprowadzone poprawnie, przy wykorzystaniu właściwych narzędzi autoryzacyjnych., mimo tego transakcji płatniczych wykonanych z konta powoda w dniu 14 stycznia 2014 r. nie można uznać za transakcje autoryzowane.

Zgodnie z art. 40 ust. 1 analizowanej ustawy, transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji w sposób przewidziany w umowie między płatnikiem a jego dostawcą, powód takiej zgody nie wyraził. Niezwłocznie powiadomił pozwanego oraz Policję, stosownie do obowiązków wynikających z art. 44 ust. 1 przywoływanej ustawy, celem wyjaśnienia przyczyn zniknięcia z konta posiadanych środków pieniężnych.

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 jedynie faktu 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.

W ocenie Sądu powód nie autoryzował transakcji, które zostały przeprowadzone bez jego wiedzy. Nie można mu również przypisać rażącego niedbalstwa w naruszeniu obowiązków, wynikających z art. 42 ustawy. Wprawdzie udostępnił on nieświadomie osobom nieuprawnionym dane przepisując na stronę internetową kod autoryzacyjny podany w treści wiadomości sms, czego nie powinien czynić, jednak nie nastąpiło to w okolicznościach świadczących o rażącym niedbalstwie z jego strony.

Powód w okresie poprzedzającym transakcje był informowany o zagrożeniach w systemach bankowości internetowej, w tym dotyczących wirusów i niebezpieczeństw związanych z ich instalowaniem, jednak zachował adekwatną staranność w dbaniu o swoje bezpieczeństwo w Internecie, gdyż korzystał z serwisu bankowego wyłącznie przez swój prywatny laptop, z legalnym oprogramowaniem, zabezpieczony należycie programem antywirusowym (co wykazał przedstawiając odpowiedni certyfikat zabezpieczeń). Nigdy nie udostępnił nikomu swojego telefonu dedykowanego jednorazowym kodom autoryzacyjnym sms, ani też go nie zagubił. Podobnie nie udostępniał nikomu swojego laptopa.

W dniu 14 stycznia 2014 r. skorzystał ze swojego prywatnego laptopa, z legalnym oprogramowaniem i zabezpieczonego programem antywirusowym, choć Bank nie stawiał swoim klientom niemal żadnych wymagań dotyczących sprzętu i oprogramowania.

W tym dniu miał problemy z wylogowaniem się z serwisu transakcyjnego Banku, gdyż strona internetowa wykazywała oznaki „zawieszania się". Podczas jednej z prób logowania się, na stronie internetowej wyświetlił się komunikat z informacją o zmianie formatu konta i prośbą o potwierdzenie zmiany kodem sms – jednocześnie na tel. komórkowy powoda dostarczona została wiadomość sms z kodem autoryzacyjnym, który przepisał on na wyświetloną stronę internetową wyglądającą w jego ocenie, jak strona do logowania się do serwisu transakcyjnego pozwanego Banku. Żądanie to, wobec faktu iż strona internetowa nie przedstawiała się jako oczywiście fałszywa, nie wzbudziło podejrzeń powoda. Tym bardziej, że po tej czynności, nie miał on żadnego problemu z ponownym zalogowaniem się do swojego konta internetowego.

Komunikat banku dotyczący tego zagrożenia, z którym zetknął się powód, został umieszczony na stronie Banku dopiero w dniu 3 lutego 2014 r., Komunikat, który wprowadził powoda w błąd pojawił się na stronie Banku (a w rzeczywistości na stronie ją imitującej), a nie w innym miejscu i okolicznościach. W ocenie Sądu, powyższe okoliczności, nie pozwalają na przypisanie powodowi rażącego niedbalstwa w związku z wpisaniem na stronie internetowej imitującej stronę Banku kodu sms służącego, co do zasady do autoryzacji transakcji, a nie do „potwierdzania zmiany formatu konta".

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 jednak płatnik doprowadził do nieautoryzowanej transakcji umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42, odpowiada on za nieautoryzowane transakcje płatnicze w pełnej wysokości (art. 46 ust. 3).

Powód w sposób niezamierzony i nieświadomy, a więc niezawiniony, dopuścił się naruszenia jednego ze swoich obowiązków ciążących na nim z mocy art. 42 ust. 2 ustawy o usługach płatniczych, za co nie może ponosić odpowiedzialności na podstawie art. 46 ust. 3 cytowanej ustawy.

W ocenie Sądu I instancji, nie istnieje niebezpieczeństwo podwójnego wyegzekwowania tej samej kwoty, gdyż ewentualne wyegzekwowanie jej od sprawcy szkody pozwoli pozwanemu bronić się odpowiednim zarzutem w drodze powództwo przeciwegzekucyjnego.

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. W myśl art. 46 ust. 1 ustawy, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej „niezwłocznie". Dopiero wynik postępowania karnego pozwolił na zbadanie i ustalenie wszystkich okoliczności sprawy, dlatego zasadne było zasądzenie odsetek od dnia wniesienia pozwu, kiedy strona pozwana miała dostateczną wiedzę pozwalającą na zwrot kwoty wskazanej w pozwie, a nie od dnia bezpośrednio po zaistnieniu zdarzenia. O kosztach orzeczono w oparciu o art. 98 k.p.c.

Apelację od wyroku wniósł pozwany Bank, który zaskarżył wyrok w części uwzględniającej powództwo.

Wniósł o zmianę wyroku poprzez oddalenie powództwa w całości oraz zasądzenie kosztów postępowania, w tym kosztów zastępstwa procesowego, na rzecz Pozwanego za l i II instancję według norm przypisanych; ewentualnie w przypadku nie podzielenia argumentów przesądzających o oddaleniu powództwa w całości wniósł o zmianę wyroku w ten sposób, aby odpowiedzialność Pozwanego, na podstawie art. 46 ust. 2 w zw. z art. 42 ust. 2 ustawy o usługach płatniczych, została ograniczona o kwotę stanowiącą równowartość w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji (na dzień 14 stycznia 2014 roku wynosił 4,1565 złotych) oraz zmianę orzeczenia o kosztach postępowania za I instancję uwzględniającą ww. modyfikację orzeczenia oraz zasądzenie od Powoda na rzecz Pozwanego kosztów postępowania, w tym kosztów zastępstwa procesowego, za II instancję według norm przypisanych ; ewentualnie w związku z zarzutem naruszenia art. 328 § 2 k.p.c. wniósł o uchylenie w całości zaskarżonego wyrok i przekazanie sprawy sądowi I instancji do ponownego rozpoznania i rozstrzygnięcia o kosztach postępowania za I i II instancję.

Zaskarżonemu wyrokowi zarzucił:

1. błąd w ustaleniach faktycznych przyjętych za podstawę wyroku:

1) poprzez przyjęcie, że Powód nie naruszył zasad bezpieczeństwa korzystania z systemów informatycznych w sposób rażący, wbrew zarzutom strony pozwanej podnoszonym w toku procesu, że działania Powoda w kontekście korzystania z bankowości elektronicznej, w szczególności w świetle obowiązków Powoda dotyczących ochrony indywidualnych środków dostępu oraz ustalonego w sprawie stanu faktycznego w zakresie zachowania Powoda, miały ostatecznie charakter rażącego niedbalstwa,

2) polegające na ustaleniu, że Powód posiadał działające aktualne oprogramowanie antywirusowe zainstalowane na komputerze, z którego korzystał logując się do systemu bankowości elektronicznej, w świetle zgromadzonego w sprawie materiału dowodowego - dokumentów, a w szczególności zeznań Powoda, z których wprost wynika, że na jego komputerze był zainstalowany wirus, a które w żaden sposób nie potwierdzają, że oprogramowanie to, nawet jeśli było zainstalowane na tym komputerze, było bieżąco aktualizowane w zakresie bazy wirusów; istotne pozostaje tu także pomięcie przez Sąd faktu sformatowania przez Powoda dysku jego komputera, co uniemożliwiło ocenę komputera pod kątem właściwych zabezpieczeń;

3) poprzez przyjęcie, że Powód nie otrzymał z Banku informacji sms weryfikującej osobnym kodem utworzenie zdefiniowanego odbiorcy (...) (na rachunek którego następnie zostały przelane środki z rachunku bankowego Powoda), która to okoliczność nie wynika z zeznań Powoda, ani nie była przez Pozwanego przyznana, a która ma istotne znaczenie dla zakresu odpowiedzialności Powoda,

4) poprzez przyjęcie, że pomimo prawidłowości wykonania transakcji z punktu widzenia systemu informatycznego Banku przy wykorzystaniu właściwych narzędzi autoryzacyjnych, kwestionowanych przez Pozwanego transakcji nie

można uznać za autoryzowaną w świetle przepisów ustawy o usługach płatniczych, co ma wpływ na odpowiedzialność Pozwanego w sprawie;

2. Niezastosowanie prawidłowej wykładni prawa krajowego w kontekście prawa unijnego, poprzez dowolne przyjęcie, że jedynie polska wersja dyrektywy jest rozstrzygająca dla prawidłowej interpretacji prawa krajowego, przyjmując, że to na stronie pozwanej leżał ciężar dowodu, że zakwestionowane transakcje płatnicze były autoryzowane przez użytkownika, podczas gdy strona pozwana wykazała, że zgodnie z prawidłową interpretacją ustawy o usługach płatniczych to na Powodzie ciąży obowiązek udowodnienia innych okoliczności, a na Pozwanym wyłącznie wykazanie, że kwestionowane transakcje, zostały w sposób prawidłowy autentyfikowane, co też uczynił,

3. Naruszenie przepisów prawa materialnego w zakresie odpowiedzialności in solidum tj. art 366 k.c. per analogiam przez wydanie wyroku zgodnie z pozwem pomimo istnienia prawomocnego wyroku karnego orzekającego obowiązek naprawienia szkody na rzecz Powoda obejmującej tą samą szkodę co dochodzona w niniejszej sprawie na podstawie innego tytułu prawnego,

4. Naruszenie art. 46 ust. 3 w związku z art. 42 ustawy o usługach płatniczych poprzez ich niezastosowanie, pomimo faktu, że z okoliczności sprawy wynika, że działania Powoda mają charakter rażącego niedbalstwa w naruszeniu zasad korzystania z instrumentu płatniczego zgodnie z umową i w sposób bezpieczny,

5. Naruszenie art. 46 ust. 2 w związku z art. 42 ustawy o usługach płatniczych poprzez ich niezastosowanie, pomimo przyjęcia, że Powód uchybił obowiązkom wymienionym w art. 42 ust. 2 przynajmniej raz udostępniając instrument płatniczy osobom nieuprawnionym poprzez wpisanie w dniu 14 stycznia 2014 roku kodu autoryzacyjnego podanego w treści sms na podstawionej stronie internetowej;

6. Naruszenie przepisów art. 481 § 1 i 2 kodeksu cywilnego w zakresie zasądzenia odsetek ustawowych za opóźnienie od dnia 1 kwietnia 2015 roku (daty wniesienia pozwu), podczas gdy ewentualny zakres odpowiedzialności pozwanego Banku może być ustalony dopiero w ramach niniejszego postępowania, w związku z czym, żądanie odsetek za opóźnienie jest niezasadne;

7. Naruszenie prawa procesowego w postaci art. 328 § 2 k.p.c. poprzez wadliwe sporządzenie uzasadnienia polegające na całkowitym pominięciu argumentów Pozwanego dotyczących błędnej interpretacji ustawy o usługach płatniczych w świetle przepisów dyrektywy oraz przyczynienia się Powoda do zaistniałej w jego majątku szkody majątkowej;

8. Naruszeniu prawa procesowego w postaci art. 233 § 1 i 2 k.p.c. poprzez dokonanie oceny dowodów w sposób wykraczający poza dopuszczalną swobodną, a więc poprzez dowolną ich interpretację. W szczególności poprzez;

1) zignorowanie zeznań Powoda w części dotyczącej:

a) wyraźnego przyznania przez niego, że na jego komputerze był zainstalowany wirus, który doprowadził do przejęcia przez osoby nieuprawnione dostępu do instrumentu płatniczego - jego indywidualnych zabezpieczeń tj. loginu i hasła,

b) przyznania przez Powoda, że udostępniając kod sms przesłany mu przez Bank do autoryzacji operacji ustanowienia zdefiniowanego (zaufanego) odbiorcy, nie zapoznał się z jego treścią wskazującą wyraźnie na przeznaczenie kodu,

które to okoliczności mają zasadnicze znaczenie dla oceny odpowiedzialności Pozwanego w sprawie;

2) uznanie, że wpisanie przez Powoda kodu sms na stronę internetową nie będącą stroną Banku, nie zabezpieczoną właściwym certyfikatem, zawierającą komunikat o zmianie formatu konta nigdy nie stosowany przez Pozwanego, i to wbrew wskazanego w wiadomości sms przeznaczeniu kodu autoryzacyjnego i wbrew przekazywanym ostrzeżeniom, nie stanowi o rażącym naruszeniu obowiązków użytkownika instrumentu płatniczego;

3) ustaleniu, wbrew zgromadzonemu w sprawie materiałowi dowodowemu, że Powód nie otrzymał z Banku informacji sms weryfikującej osobnym kodem utworzenie zdefiniowanego odbiorcy (...);

4) całkowite pominięcie dla oceny dowodów okoliczności sformatowania dysku komputera przez Powoda. Uniemożliwiło to przeprowadzenie wnioskowanego przez stronę pozwaną dowodu z opinii biegłego na okoliczność posiadania przez Powoda aktualnego i aktywnego oprogramowania antywirusowego w czasie kiedy doszło do zlecenia kwestionowanych transakcji, a co za tym idzie wykazania czy Powód dołożył wystarczającej staranności co do ciążących na nim zobowiązań korzystania z systemu bankowości internetowej w sposób prawidłowy, co najmniej w zakresie posiadania aktualnego i aktywnego oprogramowania antywirusowego,

5) nielogiczną ocenę zeznań Powoda, który z jednej strony wskazywał, że posiada legalne oprogramowanie antywirusowe, a z drugiej przyznał, że na jego komputerze musiał być zainstalowany wirus umożliwiający udostępnienie instrumentu płatniczego osobom nieuprawnionym.

W odpowiedzi na apelację powód wniósł o jej oddalenie i zasądzenie na swoja rzecz od pozwanego kosztów postępowania odwoławczego.

Sąd Apelacyjny zważył, co następuje.

Apelacja strony pozwanej okazała się w całości bezzasadna.

W pierwszej kolejności należy odnieść się do zarzutów naruszenia prawa procesowego, począwszy od naruszenia art. 328 § 2 k.p.c. poprzez wadliwe sporządzenie uzasadnienia polegające na całkowitym pominięciu argumentów pozwanego dotyczących błędnej interpretacji ustawy o usługach płatniczych w świetle przepisów dyrektywy oraz przyczynienia się powoda do zaistniałej w jego majątku szkody. Zgodnie ze wskazanym przepisem uzasadnienie wyroku powinno zawierać wskazanie podstawy faktycznej rozstrzygnięcia, a mianowicie: ustalenie faktów, które sąd uznał za udowodnione, dowodów, na których się oparł, i przyczyn, dla których innym dowodom odmówił wiarygodności i mocy dowodowej, oraz wyjaśnienie podstawy prawnej wyroku z przytoczeniem przepisów prawa. Wskazany przepis nie nakłada na sąd obowiązku odniesienia się do argumentów natury prawnej podniesionych w procesie przez strony, zarówno gdy dotyczą one wykładni prawa jak i jego zastosowania. Wyjaśnienie podstawy prawnej wyroku z przytoczeniem przepisów prawa polega na wskazaniu przepisów regulujących sporny stosunek prawny oraz na wyjaśnieniu, dlaczego w konkretnej sytuacji prawnej mają zastosowanie powołane przepisy i w jaki sposób one wpływają na rozstrzygnięcie sprawy rozpatrywanej przez sąd. Takie wyjaśnienie zawarł Sąd I instancji w uzasadnieniu zaskarżonego wyroku.

Brak jest także podstaw do podzielenia zarzutu art. 233 § 1k.p.c. Dla skuteczności zarzutu naruszenia art. 233 § 1 k.p.c. nie wystarcza stwierdzenie o wadliwości dokonanych ustaleń faktycznych, odwołujące się do stanu faktycznego, który w przekonaniu skarżącego odpowiada rzeczywistości. Konieczne jest tu wskazanie przyczyn dyskwalifikujących postępowanie sądu w tym zakresie. W szczególności skarżący powinien wskazać, jakie kryteria oceny naruszył sąd przy ocenie konkretnych dowodów, uznając brak ich wiarygodności i mocy dowodowej lub niesłusznie im je przyznając (por. postanowienie Sądu Najwyższego z dnia 23 stycznia 2001 r., sygn. akt IV CKN 970/00).

Sąd Okręgowy ustalił, że powód udostępnił osobom nieuprawnionym dane przepisując na stronę internetową, nie będącą stroną Banku, kod autoryzacyjny otrzymany w wiadomości sms, czego nie powinien uczynić.

Nie został jednak dowiedziony, ani wyjaśniony mechanizm, sugerowany przez bank, że wyświetlenie fikcyjnej internetowej strony banku, wymagało uprzedniego zainfekowania komputera powoda złośliwym oprogramowaniem (wirusem), który następnie wygenerował fałszywy komunikat z informacją o zmianie formatu konta oraz żądaniem jej akceptacji przez powoda kodem sms, a także doprowadził do przejęcia zabezpieczeń indywidualnych powoda tj. jego loginu i hasła. Ani same wyjaśnienia strony pozwanej w tym zakresie – nie mogły być uznane za udowodnienie tego faktu, ani nawet dowód z przesłuchania powoda, który zeznał: „prawdopodobnie miałem zainstalowanego wirusa" (rozprawa w dniu 30 maja 2016r.00:09:46) – mechanizmu zainfekowania laptopa powoda nie wyjaśniają.

Sąd I instancji przyjął, że sprzęt komputerowy miał zainstalowane aktualne oryginalne oprogramowanie antywirusowe firmy (...), ustalenia to oparł w tym zakresie na dowodzie z przesłuchania powoda. Pozwany podnosi,

że żaden dowód - poza gołosłownymi twierdzeniami samego powoda - nie dowodzi tego, że komputer, z którego korzystał powód był należycie zabezpieczony tj. posiadał aktualne i aktywne oprogramowanie antywirusowe, na co wystarczającym potwierdzeniem miał być już tylko fakt, że na komputerze, z którego korzystał powód doszło do zainstalowania złośliwego oprogramowania.

Zdaniem strony pozwanej dowód zakupu takiego oprogramowania nie dowodzi że program ten został zainstalowany i uruchomiony na komputerze powoda, ani, że to właśnie powód nabył to oprogramowanie, oraz że oprogramowanie to posiadało aktualną bazę wirusów umożliwiającą wykrycie złośliwego oprogramowania.

Skarżący zarzuca także, że Sąd I instancji pominął w swoich ustaleniach fakt sformatowania dysku komputera przez powoda, które uniemożliwiło dokonanie analizy i przeprowadzenie dowodu wnioskowanego przez pozwany Bank na okoliczność posiadania przez powoda aktualnego oprogramowania antywirusowego w czasie kiedy doszło do zlecenia kwestionowanych operacji. Argumentacja pozwanego jest w tym zakresie nietrafna. Jak wynika z dokonanych ustaleń po stwierdzeniu przez powoda, że jego lokaty terminowe w pozwanym banku uległy zerwaniu, a środki z rachunku w kwocie 85.000 zł przekazane zostały na nieznane konto- powód w tym samym dniu 17 stycznia 2014r. poinformował o tym zdarzeniu telefonicznie pozwany bank, a także udał się osobiście do oddziału banku, jak również w tym samym dniu o tym fakcie powiadomił organy ścigania. Gdyby pozwany wówczas poinformował powoda o konieczności zabezpieczenia dowodu w postaci komputera (laptopa), powód miałby możliwość współdziałania w tym zakresie z pozwanym. Jednak takie żądanie nie zostało wobec powoda wystosowane, ani przez bank, ani w postępowaniu prowadzonym przez policję. Pozwany bank w odpowiedzi na pisemną reklamację powoda wskazał, że nastąpiła poprawna autentyfikacja użytkownika w systemie (...), zatem nie ma podstaw do stwierdzenia nieprawidłowości operacji i tożsamości użytkownika. (pismo k. 21 akt II K 1053/14). Tym samym Bank zupełnie zbagatelizował dokonane zgłoszenie powoda i nie podjął żadnych kroków, aby zabezpieczyć dowody w sprawie, w tym laptop powoda. Pozwany nie skorzystał także z procedury zabezpieczenia dowodów przewidzianej w kodeksie postępowania cywilnego w rozdziale pt. Zabezpieczenie dowodów art. 310- 315 k.p.c.

W tej sytuacji konsekwencje braku możliwości przeprowadzenia dowodu z opinii biegłego w zakresie komputeryzacji na okoliczność braku zabezpieczenia antywirusowego komputera powoda, nie mogą obciążać powoda. To pozwany bowiem jako profesjonalista winien wykazać należytą staranność w tym zakresie. W tej sytuacji przyjęcie przez sąd I instancji, że powód zabezpieczył swój komputer programem antywirusowym, który w tym celu zakupił było uprawnione. Trudno bez narażenia się na naruszenie zasad logicznego rozumowania przyjmować, że powód kupił program antywirusowy po to, aby następnie nie instalować go na swoim komputerze. Natomiast okoliczność, że po stwierdzeniu prawdopodobnego zainfekowania laptopa wirusem powód sformatował dysk – także nie może być poczytana na jego niekorzyść. Trudno spodziewać się, aby ktokolwiek kto korzysta z komputera, po podejrzeniu o jego zainfekowanie, nie podjął żadnego działania, które miałoby na celu uniknięcie dalszych skutków ataku wirusa.

W żadnym wypadku nie może mieć w tej sytuacji zastosowania, nawet per analogiam, art. 233 § 2 k.p.c., zgodnie z którym sąd oceni jakie znaczenie nadać odmowie przedstawienia przez stronę dowodu lub przeszkodom stawianym przez nią w jego przeprowadzeniu wbrew postanowieniu sądu. Powód bowiem nie odmówił przedstawieniu dowodu, a okoliczność, że pozwany Bank pozbawiony został możliwości obrony poprzez wykazanie nieprawdziwości twierdzeń powoda, pozwany zawdzięcza własnym zaniechaniom.

Nieuprawnione jest także stwierdzenie pozwanego, że już sam przebieg zdarzenia z dnia 14 stycznia 20104r. świadczy o niewłaściwym zabezpieczeniu komputera powoda. Nie zostało bowiem po pierwsze wykazane, że powód miał zainfekowany laptop wirusem atakującym systemy bankowości elektronicznej, po drugie nie został ustalony sposób, w jaki wirus ten mógł i czy zaatakował komputer powoda, a w końcu czy aktualne wówczas na rynku programy antywirusowe, dawałyby powodowi w zakresie wirusów atakujących systemy bankowości elektronicznej poziom bezpieczeństwa w 100%, jak podnosi pozwany. Wskazane okoliczności dotyczą wiadomości specjalnych w rozumieniu art. 278 k.p.c. i nie mogą być one ustalane na podstawie przypuszczeń, własnych doświadczeń, czy też ujmowane jako fakty powszechnie znane.

Zgodnie z art. 278 § 1 k.p.c., sąd może skorzystać z opinii biegłego jako środka dowodowego w wypadkach wymagających wiadomości specjalnych. Przepis ten ogranicza samodzielność sądu w zakresie dokonywania ustaleń wymagających wiadomości specjalnych (wyrok Sądu Najwyższego z dnia 20 kwietnia 2017 r., I UK 172/16, nie publ.). Ciężar dowodu w tym zakresie obciążał stronę pozwaną, ponieważ to pozwana z faktu tego wywodziła określone skutki prawne.

Dlatego też nie można przyjąć, że została dowiedziona przez pozwanego nienależyta ochrona komputera powoda oprogramowaniem antywirusowym. Należy ponadto przypomnieć, że pozwany bank nie zaprzeczył, że nie wymagał od użytkowników bankowości internetowej instalowania na komputerach, ani telefonach komórkowych żadnego dodatkowego oprogramowania, ani certyfikatów. (k. 54 informacja Banku). W okresie kiedy doszło do zdarzenia pozwany bank nie dzwonił także do klientów w celu weryfikacji telefonicznej transakcji opiewających na wysokie kwoty.

Z dokonanych prawidłowo ustaleń wynika, że powód wpisał kod autoryzacyjny na stronie internetowej, która była łudząco podobna do strony pozwanego banku, co doprowadziło do wystawienia fałszywego komunikatu o zmianie formatu konta, tego komunikatu bank, jak wynika z jego twierdzeń, nigdy nie stosował, co zostało powiązane z żądaniem zaakceptowania komunikatu- kodem sms.

Powód potwierdził, że zatwierdził komunikat- kodem sms. Pozwany natomiast przyznał, co istotne, że kod sms, którym posłużył się powód, pochodził od Banku i był autentyczny.

Jego wysłanie przez bank było wedle pozwanego sprowokowane wirusem na komputerze powoda, który po przechwyceniu loginu i hasła klienta do bankowości internetowej wywołał w systemie banku czynność powodującą przesłanie przez bank do powoda kodu sms. Pozwany Bank zatem wysłał kod sms powodowi, który był przeznaczony do zautoryzowania operacji dodania zaufanego odbiorcy ***pomimo, że powód o przesłanie takiego kodu nigdy nie występował do Banku***. Dopiero wówczas kod udostępniony przez bank powód udostępnił osobom nieuprawnionym wpisując go w miejsce żądania zmiany formatu konta.

Należy w tym miejscu przypomnieć, że Sąd I instancji był związany, co do popełnienia przestępstwa, na mocy art. 11 k.p.c. - prawomocnym wyrokiem karnym skazującym A. N. (1). Sąd Rejonowy w Zawierciu (...) Wydział (...) wyrokiem z dnia 9 grudnia 20104r. uznał oskarżonego A. N. (1) za winnego popełnienia zarzucanego mu czynu polegającego na złamaniu zabezpieczeń elektronicznych do konta bankowego (...) S.A. o nr (...) prowadzonego dla pokrzywdzonego S. C., a następnie dodaniu swojego konta jako zidentyfikowany odbiorca, skąd po zerwaniu lokat związanych z kontem pokrzywdzonego przelał pieniądze na swoje konto zabierając w celu przewłaszczenia pieniądze w kwocie 85.000 zł na szkodę S. C., tj. przestępstwa z art. 279 § 1 kk i art. 267 § 1 kk w zw. z art. 11 § 2 kk.

Z powyższego wyroku wynika, że to nie powód, ale A. N. (2) dodał swoje konto, jako zidentyfikowanego odbiorcy do konta powoda.

Z tych względów Sąd Apelacyjny podziela ustalenia faktyczne dokonane przez Sąd I instancji z zastrzeżeniami poczynionym powyżej.

W tym stanie faktycznym nie doszło do naruszenia przez Sąd I instancji przepisów ustawy z dnia 19 sierpnia 2011r. o usługach płatniczych (Dz. U. Nr 199, poz. 1175 ze zm.).

Art.46 ust. 1 ustawy o usługach płatniczych w brzmieniu obowiązującym w dacie zdarzenia stanowi, że z zastrzeżeniem art. 44 ust. 2, 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.

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.(art. 46 ust. 3).

Powołany przepis ustala zasady odpowiedzialności dostawcy oraz płatnika w przypadku wystąpienia nieautoryzowanych transakcji, jak wynika z powołanych przepisów zakres odpowiedzialności płatnika uzależniony został od stopnia uchybienia podstawowym obowiązkom płatnika.

W świetle ust. 1 w przypadku wystąpienia nieautoryzowanych transakcji dostawca jest zobowiązany do zwrotu płatnikowi kwoty nieautoryzowanej transakcji niezwłocznie, przy czym warunkiem koniecznym jest spełnienie przez płatnika wymogów określonych w art. 44 ust. 2 u.u.p, tj. powiadomienie o nieautoryzowanych transakcjach w terminie 13 miesięcy od dnia wykonania transakcji albo obciążenia rachunku płatniczego płatnika.

Zasadą jest więc w świetle wskazanego przepisu - obowiązek zwrotu przez dostawcę kwot nieautoryzowanych transakcji. Przy czym transakcja nieautoryzowana to transakcja, na którą płatnik nie wyraził zgody w sposób wskazany w umowie.

Jeśli zatem transakcje zostały zrealizowane bez zgody płatnika oraz w okolicznościach, za które nie ponosi on odpowiedzialności, a następnie płatnik dokonał zgłoszenia wystąpienia nieautoryzowanych transakcji, to na dostawcy ciąży obowiązek zwrotu kwot nieautoryzowanych transakcji.

Jeśli jednak do nieautoryzowanych transakcji płatnik doprowadził umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia swoich obowiązków (o których mowa w art. 42 u.u.p.), wówczas to on, a nie dostawca odpowiada za nieautoryzowane transakcje.

Z art. 42 ust. 2 u.u.p. wynika, że użytkownik, z chwilą otrzymania instrumentu płatniczego, jest zobowiązany do podjęcia niezbędnych środków służących zapobieżeniu naruszeniu indywidualnych danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym.

Zdaniem Sądu Apelacyjnego prawidłowa była ocena Sądu I instancji, że brak jest podstaw do uznania, że powód wskutek rażącego niedbalstwa dopuścił się naruszenia obowiązków opisanych w art. 42.

Powód, jak była mowa, udostępnił osobom nieuprawnionym kod autoryzacyjny podany w treści wiadomości sms pochodzącej z Banku przepisując go na fikcyjną stronę internetową, czego nie powinien był czynić. Przy czym kod- pochodził z Banku i był przeznaczony do zautoryzowania operacji dodania zaufanego odbiorcy, powód o przesłanie takiego kodu nigdy do Banku nie występował. Kod ten powód dalej udostępnił osobom nieuprawnionym wpisując go w miejsce żądania zmiany formatu konta, pomimo, że kod nie był przeznaczony do tego rodzaju operacji.

Nie zostało w sprawie ustalone w jaki sposób i czy doszło do zainfekowania komputera powoda, bez specjalistycznej wiedzy z zakresu informatyki, nie sposób jest tej okoliczności ustalić, zaś dowód z opinii biegłego w zakresie informatyki nie został przeprowadzony.

Z dokonanych ustaleń wynika, że powód nie informował nikogo o swoim haśle ani loginie do konta, nie udostępniał nikomu swojego komputera, w kontaktach z serwisem internetowym Banku korzystał tylko z własnego laptopa. Komputer powoda posiadał aktywne zabezpieczenie antywirusowe, a jak już była mowa Bank nie wymagał szczególnych zabezpieczeń komputera, ze wskazaniem rodzaju oprogramowania antywirusowego w czasie zawierania umowy.

W tych okolicznościach należy przyjąć, że powód został skłoniony podstępnie przez osobę nieuprawnioną do udostępnienia tej osobie danych tj. kodu autoryzacyjnego sms, pochodzącego z banku, w związku z tym nie sposób mu przypisać rażącego niedbalstwa, a co najwyżej można mu przypisać niezachowanie należytej staranności- tj. zwykłe

niedbalstwo. Niedbalstwo, będące postacią winy nieumyślnej, zachodzi wówczas, gdy sprawca w ogóle nie wyobraża sobie skutku swojego zachowania, choć może i powinien go sobie wyobrazić. Choć z drugiej strony nawet gdyby powód przeczytał wiadomość sms z Banku niekonieczne – wiedziałby, że nie dotyczyła ona autoryzacji operacji zmiany formatu konta. Wedle twierdzeń pozwanego informacja sms pochodzą z Banku zawierała w swej treści stwierdzenie: „Operacja dot. odbiorcy nazwa: (...) (sms - k. 252v). W treści sms z Banku nie ma mowy o operacji ***dodania zaufanego odbiorcy***, ale enigmatyczne stwierdzenie, że operacja dot. odbiorcy o nazwie (...).

Rażące niedbalstwo (culpa lata) - to wyższy stopień winy nieumyślnej. Przyjmuje się, że chodzi tu o niezachowanie staranności, jakiej można by wymagać od osób najmniej nawet rozgarniętych. Kodeks cywilny posługuje się tym pojęciem w odniesieniu do dłużnika w przepisach przykładowo: art. 777 § 1 k.c., 788 § 1 i 3 k.c., 891 § 1 k.c., w odniesieniu do wierzyciela: 826 § 3 k.c., 827 § 1 k.c.

Trudno jest przypisać w tej sytuacji rażące niedbalstwo powodowi– skoro dane zostały od niego podstępnie wyłudzone, w okolicznościach, które mogły u powoda wzbudzić fałszywe przekonanie, że postępuje on w sposób prawidłowy, przy enigmatycznym oznaczeniu transakcji, której dedykowany był kod do autoryzacji.

Nie można także zgodzić się z twierdzeniami apelacji, że powód winien posiadać wiedzę o aktualnych zagrożeniach hakerskich, skoro pozwany Bank wiedzy o takich metodach działania oszustów komputerowych w owym czasie także nie posiadał. Jest bezsporne, że komunikaty o tego rodzaju zagrożeniach pojawiały się na stronie Banku dopiero po zdarzeniu z udziałem powoda.

Trafnie także ocenił Sąd I instancji, że powód nie autoryzował transakcji, które zostały przeprowadzone bez jego wiedzy.

Przepisy ustawy na dostawcę nakładają ciężar dowodu, że transakcja płatnicza została autoryzowana przez płatnika, przy czym samo wykazanie faktu zarejestrowania (czyli wykazanie, że doszło do prawidłowej autoryzacji transakcji płatniczej) jeszcze nie oznacza, że transakcja została autoryzowana przez płatnika. Na co wskazuje regulacja zawarta w art.45 ust. 1 ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. 2. 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.

Ze wskazanego przepisu wynika, że dostawca powinien udowodnić i wskazać dowody, inne niż zarejestrowana prawidłowo autoryzacja, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji albo ***wskutek rażącego niedbalstwa naruszył co najmniej jeden z obowiązków określonych w art. 42***.

Powód, jak zostało wykazane nie autoryzował dokonanych transakcji. W rozpoznawanej sprawie została ustalona osoba, która autoryzacji, zamiast powoda, dokonała. Jest to skazany A. N. (1), który złamał zabezpieczenia elektroniczne do konta bankowego powoda, następnie dodał swoje konto jako zidentyfikowanego odbiorcy, aby po zerwaniu lokat związanych z kontem powoda przelać pieniądze na swoje konto pieniądze w kwocie 85.000 zł na szkodę powoda.

Jeżeli transakcja płatnicza jest autoryzowana, oznacza to, że zgodę na transakcję wyraził sam płatnik, nie jest zatem autoryzowaną taka transakcja, której dokonano przy użyciu instrumentu płatniczego należącego do płatnika ale bez jego zgody, tak jak w rozpoznawanej sprawie.

Skarżący wskazuje także i na to, że nie mogą go obciążać błędy popełnione przez Rzeczpospolitą Polską w zakresie implementacji dyrektywy 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, 2002/65/WE, 2005/60/WE i

2006/48/WE i uchylająca dyrektywę 97/5/WE. Sąd Apelacyjny podziela pogląd, że przepisy prawa wspólnotowego muszą być interpretowane z uwzględnieniem wszystkich wersji językowych, a nie tylko w brzmieniu podanym w języku polskim w Dzienniku Urzędowym Unii Europejskiej. Pozwany nie zgłosił jednak dowodów na okoliczność zarzucanej nieprawidłowości tłumaczenia polskiej wersji językowej aktu prawa Unii Europejskiej, ani nie wnioskował o porównanie jej z innymi wersjami językowymi, co niewątpliwie powodowałoby konieczność skorzystania z pomocy tłumaczy, a być może biegłych.

Poza tym podzielając tok rozumowania pozwanego – odpowiedzialność banku w przypadku przywłaszczenia przez osobę nieuprawnioną instrumentu płatniczego w zasadzie zawsze byłaby wyłączona. Skarżący wskazuje, że odpowiedzialności banku powinna być ocenia przez pryzmat postanowień Dyrektywy, w szczególności jej art, 59 ust. 1. Bank w celu udowodnienia, że klient autoryzował transakcję, zobowiązany byłby wyłącznie dowieść, że transakcja była autentykowana (uwierzytelniona), odpowiednio zapisana, wprowadzona do ksiąg i nie zakłócona przez awarię techniczną lub inny defekt. Bank nie miałby obowiązku udowodnienia autoryzacji, ale „autentykacji" (uwierzytelnienia), przez co należy rozumieć procedurę pozwalającą bankowi na sprawdzenie użycia konkretnego instrumentu płatniczego, w tym jego indywidualnych zabezpieczeń.

W takiej sytuacji nawet skazanie wyrokiem karnym bezpośredniego sprawcy szkody- pozwalałoby dowieść bankowi, że transakcja taka, przy wykorzystaniu skradzionego instrumentu płatniczego, została prawidłowo wykonana przez bank, po jej uwierzytelnieniu. Odpowiedzialność banku byłaby w zasadzie ograniczona do transakcji zakłóconych jedynie przez awarię techniczną, czy inny defekt. Nie jest to na gruncie tak dyrektywy, jak i ustawy o usługach płatniczych – pogląd możliwy do przyjęcia. Skarżący pomija ust. 2 art. 59 Dyrektywy, który stanowi, że w przypadku gdy użytkownik usług płatniczych zaprzecza temu, że autoryzował wykonaną transakcję płatniczą, zarejestrowane przez dostawcę usług płatniczych samo użycie instrumentu płatniczego niekoniecznie jest wystarczające do udowodnienia, że transakcja płatnicza została przez płatnika usług płatniczych autoryzowana albo że płatnik działał w nieuczciwych zamiarach lub dopuścił się celowego lub rażącego zaniedbania co najmniej jednego z obowiązków przewidzianych w art. 56.

Przypomnieć należy, że celem przyjętych w Dyrektywie rozwiązań było doprowadzenie do utworzenia ram prawnych jednolitego rynku usług płatniczych w UE. W preambule dyrektywy jest mowa, że konsumenci i przedsiębiorstwa nie są w takiej samej sytuacji, nie potrzebują takiego samego poziomu ochrony. Dlatego ważne jest zagwarantowanie praw konsumenta przepisami, od których nie można odstąpić w umowie (pkt 20). Aby ocenić ewentualne zaniedbanie ze strony użytkownika usług płatniczych, należy 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).

Brak jest także podstaw do podzielenia zarzutów apelacji, aby uznać odpowiedzialność powoda za nieautoryzowane transakcje przynajmniej w zakresie wynikającym z art. 46 ust. 2 u.u.p.

Zgodnie z art. 46 ust. 2 w brzmieniu obowiązującym w dacie zdarzenia: 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, jeżeli nieautoryzowana transakcja jest skutkiem:

1) posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub

2) przywłaszczenia instrumentu płatniczego lub jego nieuprawnionego użycia w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2."

Z dokonanych ustaleń wynika, że zakwestionowane transakcje płatnicze zostały dokonane na skutek nieuprawnionego użycia przez płatnika w okolicznościach omówionych powyżej, a następnie kradzieży instrumentu płatniczego. Trudno

powoda obciążać odpowiedzialnością za ową kradzież, skoro powód nie miał nawet możliwości stwierdzenia tej kradzieży, a dokonane transakcje płatnicze zostały dokonane w krótkim czasie po owej kradzieży - bez jego wiedzy i zgody.

Z tych także względów brak było podstaw do podzielenia zarzutu przyczynienia się powoda do szkody w rozumieniu art. 362 k.c. Zachowaniu powoda, jak była mowa nie można przypisać rażącego niedbalstwa, a przyjęte zwykłe niedbalstwo – dodatkowo w okolicznościach sprawy opisanych wyżej, nie uzasadnia przyczynienia się powoda i w rezultacie obniżenia dochodzonej kwoty w żadnym zakresie.

Brak jest także podstaw do stwierdzenia zarzucanego naruszenia prawa materialnego w zakresie odpowiedzialności in solidum tj. art 366 k.c. per analogiam przez wydanie wyroku, pomimo istnienia prawomocnego wyroku karnego orzekającego obowiązek naprawienia szkody na rzecz powoda obejmującej tą samą szkodę co dochodzona w niniejszej sprawie na podstawie innego tytułu prawnego.

Zarzut ten jest całkowicie bezzasadny. Po pierwsze sam fakt wydania wyroku karnego orzekającego obowiązek naprawienia szkody na rzecz powoda- nie oznacza przecież, że szkoda to zostanie przez skazanego A. N. (1) (nota bene- osoby bezdomnej) naprawiona. Po drugie trafnie Sąd I instancji wskazał, że nie istnieje niebezpieczeństwo podwójnego wyegzekwowania roszczenia z uwagi na możliwość obrony powództwem przeciwegzekucyjnym. Po trzecie wyrok zasadzający nie mógł zastrzegać tego rodzaju odpowiedzialności pozwanego (in solidum), skoro powód nie zgłosił takiego żądania. Z kolei brak, tak sformułowanego żądania, w żaden sposób nie uzasadniał oddalenia powództwa wprost w całości, jak podnosi się w apelacji, skoro żądanie powoda było uzasadnione merytorycznie.

Niezasadny okazał się także zarzut naruszenia art. 481 k.c. Sąd I instancji zasądził odsetki ustawowe od dnia wniesienia pozwu.

W myśl art. 46 ust. 1 ustawy, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej niezwłocznie. Skoro wskazany przepis wskazuje termin spełnienia świadczenia Banku, niezwłocznie po stwierdzeniu wystąpienia nieautoryzowanej transakcji, nie można zgodzić się z pozwanym, że odsetki miałyby zostać zasądzone dopiero od dnia uprawomocnienia się wyroku zasądzającego szkodę na rzecz powoda.

Z podniesionych względów apelacja jako bezzasadna podlegała oddaleniu. O kosztach Sąd Apelacyjny orzekł na podstawie art. 98 § 1 i 3 k.p.c. w z. z art. 391 § 1 k.p.c. Koszty te obejmują jednokrotne wynagrodzenie pełnomocnika powoda, obliczone według stawki wskazanej w § 2 pkt 6 w zw. z § 10 ust. 1 pkt 2 Rozporządzenia Ministra Sprawiedliwości w sprawie opłat za czynności adwokackie z dnia 22 października 2015r. (Dz. U. z 2016r., poz. 1668). Brak było podstaw do przyznania wynagrodzenia w podwójnej stawce, w postępowaniu apelacyjnym odbyła się tylko jedna rozprawa, zaś niezbędny nakład pracy adwokata nie wykraczał poza przeciętny w tego rodzaju sprawach, a zatem nie może być uznany za uzasadniający podwyższenie stawki do dwukrotności stawki minimalnej, to samo dotyczy wkładu pracy adwokata w przyczynienie się do wyjaśnienia okoliczności faktycznych i prawnych na etapie postępowania odwoławczego, natomiast żądanie zwrotu kosztów podróży nie zostało w żaden sposób przed sądem odwoławczym wykazane, dlatego także nie mogło zostać uwzględnione.