Sygn. akt I ACa 1174/16

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 10 marca 2017 r.

Sąd Apelacyjny w Łodzi I Wydział Cywilny w składzie:

Przewodniczący: SSA Bożena Wiklak

Sędziowie: SA Anna Miastkowska (spr.)

del. SO Ryszard Badio

Protokolant: st. sekr. sąd. Grażyna Michalska

po rozpoznaniu w dniu 10 marca 2017 r. w Łodzi na rozprawie

sprawy z powództwa ***L. S. i B. S.***

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

o zapłatę

na skutek apelacji strony pozwanej

od wyroku Sądu Okręgowego w Łodzi

z dnia 9 maja 2016 r. sygn. akt II C 1284/14

I. ***oddala apelację;***

II. ***zasądza od (...) Spółki Akcyjnej w W. na rzecz L. S. i B. S. kwotę 5.400 (pięć tysięcy czterysta) zł tytułem zwrotu kosztów zastępstwa procesowego w postępowaniu apelacyjnym.***

Sygn. akt I ACa 1174/16

UZASADNIENIE

Zaskarżonym wyrokiem z dnia 9 maja 2016 r. Sąd Okręgowy w Łodzi, w sprawie z powództwa L. S. i B. S., przeciwko (...) Spółce Akcyjnej z siedzibą w W. o zapłatę, zasądził od pozwanej solidarnie na rzecz powodów kwotę 104.309,04 zł z ustawowymi odsetkami i kosztami procesu, oddalając powództwo w pozostałym zakresie.

Powyższe orzeczenie zostało oparte na ustaleniach, które Sąd Apelacyjny podzielił i uznał za własne.

Sąd I instancji zaznaczył między innymi, że powodowie zawarli z pozwanym – działającym wówczas po nazwą (...) Bank Spółka Akcyjna z siedzibą w W. (...) Oddział Bankowości Detalicznej w Ł. dwie umowy z dnia 18 września 2008 r. o prowadzenie rachunku oszczędnościowo- rozliczeniowego, na podstawie której otwarte zostało wspólne konto (...) o numerze (...) i o prowadzenie rachunku oszczędnościowo (...) o numerze (...). oraz umowę z dnia 6 marca 2009 r. o świadczenie usług bankowych w MultiBanku.

Stosunki wynikające z tych umów, zgodnie z ich postanowieniami, były kształtowane przez stanowiące ich integralną część regulaminy otwierania i prowadzenia rachunków oszczędnościowo – rozliczeniowych i oszczędnościowych.

W dniu 11 kwietnia 2013 r. uległa zmianie nazwa pozwanego z (...) Bank Spółka Akcyjna z siedzibą w W. na (...) Spółka Akcyjna z siedzibą w W..

Powodowie korzystali z usług bankowości elektronicznej MultiBanku.

W dniu 4 lipca 2013 r. powód dokonywał transakcji przy użyciu tej usługi. Rozpoczął proces logowania do bankowego systemu elektronicznego za pośrednictwem strony internetowej pozwanego - wpisał swój login, hasło i wcisnął przycisk „zatwierdź". W momencie gdy zalogował się do banku, na ekranie jego komputera, na półprzezroczystym tle MultiBanku pojawił się komunikat, którego powód nie miał możliwości zamknięcia. W treści komunikatu zwarto informację, że w celu poprawy jakości i bezpieczeństwa należy dokonać zainstalowania w telefonie odpowiedniego oprogramowania – (...). Powód postąpił zgodnie z instrukcją w komunikacie i zainstalował żądaną aplikację. W trakcie tego procesu podał m.in. numer swojego telefonu. Następnie wykonał przelew na kwotę 85,12 zł na poczet opłaty za gaz. Po otrzymaniu informacji, że przelew został dokonay, powód wylogował się z systemu bankowości elektronicznej. Przez kilka kolejnych dni powód nie logował się do systemu bankowości elektronicznej pozwanego.

W dniu 5 lipca 2013 r. z rachunku oszczędnościowego powoda (...) o numerze (...) na wspólny rachunek oszczędnościowo- rozliczeniowego powodów o numerze (...) przelano dwie kwoty: 80.150 zł i 20.000 zł. Następnie w tym samym dniu wspólny rachunek oszczędnościowo – rozliczeniowego powodów o numerze (...) został obciążony na rzecz posiadaczy rachunków o numerach: (...)) (...) posługującego się nazwiskiem A. M. kwotą 29.874 zł; 2) (...), posługującego się nazwiskiem M. G. kwotą 29.769 zł; 3) (...), posługującego się nazwiskiem P. D. kwotą 29.385 zł; 4) (...), posługującego się nazwiskiem A. M. kwotą 25.874 zł. (ta ostatnia kwota została tego samego dnia zwrócona na wspólny rachunek oszczędnościowo – rozliczeniowego powodów o numerze (...) i została ponownie przelana na rachunek o numerze (...)); 5) (...) posługującego się nazwiskiem P. D. kwotą 29.385 zł. W dniu 7 lipca 2013 r. ze wspólnego rachunku oszczędnościowo – rozliczeniowego powodów wykonano 25 przelewów po 1.000 zł każdy z nich na rzecz posiadacza rachunku o numerze (...) tytułem wpłaty dla serwisu (...) zakup kuponów U-cash.

W dniu 7 lipca 2013 r. dokonano 8 przelewów z karty kredytowej powoda V. A. po 1.000 zł każdy z nich.

Powodowie nie autoryzowali powyższych transakcji.

W dniu 9 lipca 2013 r. powódka przy próbie zapłaty kartą za zakupy na stacji benzynowej uzyskała informację o braku środków na koncie. O fakcie tym poinformowała powoda, który z kolei zadzwonił na infolinię Banku w celu uzyskania informacji. Tego samego dnia powód udał się też do placówki Banku w B. i poprosił o wydruk ostatnich operacji. Na jego podstawie stwierdził na koncie ok. 30 operacji zrealizowanych bez jego autoryzacji. W związku z tym złożył reklamację i poinformował Bank o zaistniałej sytuacji.

Tego samego dnia powód zgłosił również zawiadomienie o podejrzeniu popełnienia przestępstwa na jego szkodę na Komendzie Miejskiej Policji w P.. W jego wyniku zostało wszczęte śledztwo przez Prokuraturę Rejonową w Tarnowskich Górach Ośrodek (...) w P., prowadzone pod sygnaturą 5 Ds/423/13. Dotyczyło ono nieautoryzowanych przelewów z rachunków bankowych na szkodę powoda, ale także na szkodę innych klientów strony pozwanej. Obecnie postępowanie w tej sprawie prowadzi Prokuratura Apelacyjna w Krakowie Wydział V do Spraw Przestępczości Zorganizowanej i Korupcji pod sygnaturą Ap V Ds. 42/13/Sp.

W 2013 r. zdarzyły się liczne przypadki wyprowadzenia środków z rachunków bankowych klientów strony pozwanej w całej Polski. W ok. 100 przypadkach ustalono ten sam mechanizm przejęcia kontroli nad kontem klienta. W pierwszej kolejności następowała infekcja komputera. Szkodliwe oprogramowanie „wstrzykiwało" kod, który nakładał fałszywą stronę na właściwą stronę internetową pozwanego banku. Strona ta przypominała stronę banku. Adres strony internetowej wskazywał na stronę banku, znajdowało się tam logo banku, jednakże zawartość takiej strony nie była banku. Przy logowaniu klienta do serwisu transakcyjnego fałszywa strona generowała komunikat informujący o konieczności zwiększenia bezpieczeństwa rachunku poprzez konieczność zainstalowania konkretnego certyfikatu na telefonie komórkowym klienta. Następnie klient wybierał odpowiednie dla systemu operacyjnego

telefonu oprogramowanie (np. android), po którego wybraniu pojawiało się okienko do wprowadzenia numeru telefonu komórkowego, na który miały być przesłane dalsze instrukcje do instalacji domniemanego certyfikatu. Klient banku otrzymywał SMS-a z linkiem, po wybraniu którego miała nastąpić instalacja certyfikatu. Ponieważ certyfikat pochodził z zewnątrz, na wyświetlaczu telefonu pojawiał się komunikat „nie zaufane źródło", który trzeba było zaznaczyć w telefonie. Użytkownik ponownie otrzymywał komunikat, że przejmuje wszelką odpowiedzialność. Po potwierdzeniu komunikatu o nie zaufanych źródłach istniała możliwość zainstalowania z zewnętrznych źródeł wszelkich dodatkowych aplikacji. Tylko od użytkownika zależała aprobata potwierdzenia. Klient musiał zatwierdzić komunikat o treści: zezwalaj na instalacje aplikacji z nie zaufanych źródeł. Wówczas następowała instalacja certyfikatu. Gdy klient przeszedł całość procedury wyświetlaną przez szkodliwe oprogramowanie, użytkownik miał możliwość dalszego korzystania z serwisu transakcyjnego. Użytkownik pozostawał dalej na stronie banku.

W pozwanym banku klient otrzymywał kod SMS w momencie wykonywania operacji. Od momentu instalacji szkodliwego oprogramowania na telefonie komórkowym, wykonywanie operacji przez klienta nie było możliwe, nie dochodziły bowiem SMS-y z banku. Bank nie weryfikował telefonu i aplikacji.

Komputer powoda posiadał aktywne, aktualne zabezpieczenia antywirusowe - program antywirusowy M. E. i zaporę systemową. Skuteczność zainstalowanego przez powoda oprogramowania była niska. (...) ten zapewnia tylko podstawową ochronę i zaleca się używanie innego oprogramowania. Z punktu widzenia informatycznego żaden program antywirusowy, nawet przodujący w rankingach, nie daje 100 % skuteczności.

Na dysku powoda ujawniono pliki programu identyfikowanego przez systemy antywirusowe jako trojan. Ujawniony wirus umożliwiał przejęcie pełnej kontroli nad zainfekowanym komputerem poprzez modyfikację obszarów pamięci operacyjnej fizycznej. W wyniku infekcji możliwe było przejęcie danych dostępowych do konta bankowego i wysłanie ich za pośrednictwem internetu atakującemu. Infekcja nastąpiła 2 lipca 2013 r. W dniu 4 lipca 2013 roku nastąpiło logowanie z komputera powoda, za pośrednictwem strony internetowej, do konta banku (...). W trakcie tego logowania wirus przechwycił dane dostępowe do konta bankowego, użyte później do kradzieży środków pieniężnych z konta. Drugim etapem ataku było zainstalowanie w telefonie aplikacji E-security. Zainstalowane przez użytkownika w telefonie oprogramowanie, umożliwiło przejęcie pełnej kontroli nad urządzeniem, manipulowanie wiadomościami SMS. W tego typu atakach blokowane są powiadomienia o przychodzących wiadomościach SMS z banku (są one niewidoczne dla użytkownika telefonu), oraz umożliwia przesłanie wiadomości SMS bez wiedzy użytkownika na wskazany numer. Funkcjonalność ta umożliwia wykorzystanie oprogramowania E-security do przeprowadzania nieautoryzowanych transakcji przez osoby uprawnione operacji bankowych (autoryzowanych kodem wysyłanym przez wiadomość SMS). Sposób zabezpieczenia danych z telefonu nie pozwolił na dotarcie do śladów działania tego oprogramowania.

Z punktu widzenia informatycznego nie było przesłanek pozwalających na stwierdzenie, że został przełamany system komputerowy MultiBanku, bądź jego system zabezpieczeń. Z punktu widzenia banku identyfikacja klienta jak i autoryzacja transakcji przebiegała zgodnie z procedurą - logowanie do portalu bankowego nastąpiło przy użyciu właściwego loginu i hasła z wykorzystaniem szyfrowanego połączenia, kod autoryzacji transakcji został wysłany wiadomością SMS na wskazany numer telefonu, a następnie wprowadzony w portalu internetowym.

W pozwanym Banku poprawność transakcji jest weryfikowana. Jest konieczność potwierdzania hasłem SMS lub listą haseł z papierowej listy. Hasła wysyłane są SMS-em na numer telefonu klienta. Klient wprowadzając wiadomość SMS jednoznacznie potwierdza chęć wykonania danego przelewu. Dalsze weryfikacje nie są przez Bank wykonywane. Bank nie sprawdza kodu IP nieautoryzowanych transakcji. Każdy klient z każdego miejsca na świecie może się zalogować. Hasło jest wygwiazdkowane. Klucz autoryzacji nie wymusza na kliencie zmiany hasła co jakiś czas.

Powodowie nie informowali nikogo o swoim haśle ani loginie do konta. Nie było włamania do miejsca zamieszkania powodów. Powodowie nie korzystali z przelewów dotpay, nie kupowali kuponów E cash. Kartą kredytową zwykle płacili za zakupy. Nie dokonywali przelewów z karty kredytowej. Na komputerze, na którym się logował powód nie korzystał z opcji zapamiętywania hasła dostępu do konta. Powód nie miał uruchomionej usługi powiadomienia SMS-

ami o transakcjach. Powodowie nie znają osób na rzecz których zostały przelane środki z ich konta i nie dokonywali jakichkolwiek przelewów w dniach od 5 do 9 lipca 2013 r.

Pozwany Bank zamieszczał na stronach internetowych mBanku ostrzeżenia przed podawaniem przez klientów danych umożliwiających dostęp do ich rachunków bankowych. Ostrzeżenia dotyczyły m.in. komunikatów, których szata graficzna oraz treść zostały tak przygotowane, aby do złudzenia przypominały serwis Banku. Informowano też o programach, między innymi w dniu 20 maja 2013 r., które mogą zagrażać telefonowi, m.in. o certyfikacie e-security. Ostrzeżenia te były aktualizowane, gdy pojawiało się bądź zmieniało zagrożenie.

Na stronie logowania M., z którego serwisu internetowego korzystali powodowie nie było takich informacji. Bank nie wskazywał z jakiego oprogramowania antywirusowego klienci powinni korzystać.

Pomiędzy powodem, a bankiem prowadzona była korespondencja w związku z postępowaniem reklamacyjnym. Roszczenia powoda nie zostały w większości uwzględnione. Bank pokrył straty jedynie z tytułu użycia kart kredytowych i debetowych. W dniu 19 sierpnia 2013 r. wyrównał kwoty wykorzystanych produktów kredytowych – kredytu odnawialnego oraz karty kredytowej –rachunek M. A., który został uznany kwotą 7.685,76 zł, a karta kredytowa V. A. kwotą 9.815,82 zł.

Pozwany nie wyraził zgody na postępowanie mediacyjne przed Sądem Polubownym przy Komisji Nadzoru Finansowego.

Wydając powyższy wyrok Sąd I instancji uznał, że powództwo było usprawiedliwione co do zasady i w przeważającej mierze także co do wysokości. Roszczenie powodów znalazło oparcie w przepisach ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (t. jedn. Dz. U. z 2014 r., poz. 873 ze zm.), która 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).

Strony niniejszego postępowania umówiły się, że zgoda na wykonanie transakcji płatniczych za pośrednictwem usług bankowości elektronicznej świadczonych przez pozwany Bank będzie przez powodów udzielana za pośrednictwem kanałów dostępu, określonych w regulaminach po dokonaniu ich aktywacji, m.in. strony internetowej banku po zalogowaniu się do konta za pomocą danych identyfikacyjnych i haseł do kanałów dostępu. Na pozwanym 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 powodach natomiast - jako użytkownikach 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 nie udostępniania go osobom nieuprawnionym (art. 42 ust. 2).

Sąd I instancji podkreślił, że 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, powodowie natomiast swoim obowiązkom wymienionym w art. 42 ust. 2 ustawy uchybili na skutek udostępnienia instrumentu płatniczego osobom nieuprawnionym przez zainstalowanie przez powoda w telefonie oprogramowania, umożliwiającego przejęcie kontroli nad urządzeniem, a co za tym idzie manipulowanie wiadomościami SMS, łącznie z kodami dostępu. Powód uczynił to w sposób niezamierzony i nieświadomy.

Udostępnienie przez powoda za pośrednictwem podstawionej witryny internetowej swoich danych identyfikacyjnych oraz hasła z listy będącego w jego posiadaniu osobom nieuprawnionym o nieustalonej tożsamości umożliwiło tym osobom zalogowanie się do konta powoda i wykonanie szeregu, wskazanych wcześniej transakcji. Czynności te, z punktu widzenia systemu informatycznego Banku były przeprowadzone poprawnie, przy wykorzystaniu właściwych

narzędzi autoryzacyjnych. Mimo tego transakcji płatniczych wykonanych z konta powodów w dniach od 5 do 7 lipca 2013 r. nie można było uznać, zdaniem Sądu, za transakcje autoryzowane w rozumieniu art. 40 ust. 1 ustawy. Powodowie nie wyrazili zgody na dokonanie transakcji o czym świadczył fakt, że niezwłocznie powiadomili stronę pozwaną oraz Policję, stosownie do obowiązków wynikających z art. 44 ust. 1 ustawy, celem wyjaśnienia przyczyn zniknięcia z konta niemal całych posiadanych oszczędności.

Sąd nadto zaznaczył, 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 tegoż przepisu.

W ocenie Sądu Okręgowego, w okolicznościach niniejszej sprawy nie można było przypisać powodom zgody ani woli podjęcia czynności zmierzających do przeprowadzenia kwestionowanych transakcji płatniczych przy użyciu posiadanych przez nich instrumentów płatniczych, a które to okoliczności świadczyłyby o autoryzowaniu przez nich transakcji. W przypadku powódki nie wystąpiło jakiekolwiek uchybienie odnośnie udostępnienia instrumentu płatniczego osobom nieuprawnionym, a obojgu powodom nie można było też przypisać umyślnego doprowadzenia do nieautoryzowanych transakcji płatniczych, gdyż o ich dokonaniu dowiedzieli się przypadkiem.

Zdaniem Sądu, powodowie nie dopuścili się również rażącego niedbalstwa w naruszeniu obowiązków wynikających z art. 42 ustawy. Wprawdzie powód w istocie umożliwił osobom nieuprawnionym dostęp do konta, czego nie powinien czynić, ale nie nastąpiło to w okolicznościach świadczących o rażącym niedbalstwie z jego strony. Do zainfekowania komputera użytkownika usług bankowości elektronicznej może dojść w podstępny, lecz prosty sposób. Powód w okresie poprzedzającym kwestionowane transakcje nie otrzymał żadnej wiadomości dotyczącej bezpośrednio kont w pozwanym Banku. Powodowie nie informowali nikogo o swoim haśle ani loginie do konta. Nie było włamania do miejsca zamieszkania powodów. Na komputerze z którego logował się powód nie korzystał z opcji zapamiętywania hasła dostępu do konta. W dniu 4 lipca 2013 r. przy dokonywaniu transakcji powód usiłował zalogować się na stronie internetowej M.. Po rozpoczęciu procesu logowania do bankowego systemu elektronicznego za pośrednictwem strony internetowej pozwanego, na ekranie jego komputera, na tle MultiBanku pojawił się komunikat, którego nie można było zamknąć. W treści komunikatu zawarto informację, że należy dokonać określonych czynności w celu poprawy jakości i bezpieczeństwa. Żądanie to, wobec trudności z uzyskaniem połączenia, mogło przedstawiać się wiarygodnie. Powód postąpił zgodnie z instrukcją zawartą w komunikacie. Dopiero po tym mógł dokonać zamierzonej transakcji i wylogować się z systemu bankowości elektronicznej. Nadto komputer powoda posiadał aktywne, aktualne zabezpieczenia antywirusowe i włączoną zaporę systemową. W ocenie Sądu, fakt, że skuteczność zainstalowanego przez powoda oprogramowania była niska albowiem system ten zapewniał tylko podstawową ochronę, nie miała znaczenia o tyle, że strona pozwana nie wykazała, aby stawiała swoim klientom jakiekolwiek wymagania dotyczące sprzętu czy oprogramowania. Z drugiej strony, jak wskazał biegły, z punktu widzenia informatycznego żaden program antywirusowy, nawet przodujący w rankingach, nie dawał 100% skuteczności.

Strona pozwana podnosiła wprawdzie, że na stronach internetowych mBanku były umieszczane ostrzeżenia przed podawaniem przez klientów danych umożliwiających dostęp do ich rachunków bankowych oraz przed możliwością pojawienia się m.in. szaty graficznej do złudzenia przypominającej stronę Banku, jak również ostrzeżenia o programach, które mogą zagrażać telefonowi m.in. o certyfikacie e-security i możliwym, przedmiotowym schemacie działania przestępców, jednakże strona ta nie wykazała, aby komunikaty takie były na stronach internetowych Banku, z których korzystali powodowie. Powodowie załączyli natomiast wydruki z serwisu internetowego mBanku, na których takich informacji nie było.

Ponadto ofiarą ataku cyberprzestępców padli nie tylko powodowie, ale znaczna liczba innych klientów pozwanego Banku. Okoliczność ta przemawiała za tym, że strona z której korzystał powód w dniu 4 lipca 2013 r. nie przedstawiała się jako oczywiście fałszywa.

Sąd Okręgowy wskazał także na brak reakcji strony pozwanej na dokonywane na kontach powodów operacje. Transakcje jakich powodowie dokonywali wcześniej sprowadzały się bądź do opłat za media, bądź za zakupy. Nagła ilość transakcji i to – w przypadku kart – o podobnej wartości winna wzmóc czujność banku jako profesjonalisty i winna spowodować reakcję w postaci żądania dodatkowego ich potwierdzenia, co nie miało miejsca.

Powyższe okoliczności spowodowały, że Sąd nie przypisał powodom rażącego niedbalstwa.

Z uwagi jednakże na fakt, że powodowie w sposób niezamierzony i nieświadomy dopuścili się, obiektywnie rzecz ujmując, naruszenia jednego ze swoich obowiązków ciążących na nim z mocy art. 42 ust. 2 ustawy o usługach płatniczych, Sąd I instancji uznał, że winni ponieść odpowiedzialność za nieautoryzowane przelewy z konta do wysokości 150 euro, wyrażonej z złotych.

Z tytułu opóźnienia w zwrocie zasądzonej wyrokiem kwoty, powodom należały się odsetki w wysokości ustawowej zgodnie z art. 481 § 1 i 2 k.c.

O kosztach orzeczono w oparciu o art. 100 k.p.c. przy przyjęciu, że powodowie wygrali proces w 99%.

Apelację od powyższego wyroku wywiodła strona pozwana, zarzucając:

1. nierozpoznanie istoty sprawy poprzez niezbadanie przez Sąd I instancji podnoszonego przez pozwanego zarzutu przyczynienia się powodów do powstania szkody, której naprawienia powodowie dochodzą w przedmiotowej sprawie;

2. naruszenie prawa procesowego, tj:

a) art. 233 § 1 k.p.c. poprzez dokonanie jednostronnej oceny dowodów w sposób nie wszechstronny, a także sprzeczny z zasadami doświadczenia życiowego oraz logicznego rozumowania, polegający w szczególności na:

- sprzecznym z treścią zgromadzonego w sprawie materiału dowodowego przyjęciu, że powodowie nie wykazali się w sprawie rażącym niedbalstwem w zakresie ochrony dostępu do swojego rachunku bankowego wbrew treści zeznań powoda, treści sporządzonej w postępowaniu opinii biegłego oraz uzupełniającego przesłuchania biegłego,

- przyjęciu przez Sąd I instancji pełnej odpowiedzialności pozwanego mimo, że w zaskarżonym wyroku Sąd uznał, że pozwany wywiązywał się z obowiązku zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, powodowie natomiast swoim obowiązkom wymienionym art. 42 ust. 3 ustawy o usługach płatniczych uchybili na skutek udostępnienia instrumentu płatniczego osobom nieuprawnionym przez zainstalowanie przez powoda w telefonie oprogramowania umożliwiającego przejęcie kontroli nad urządzeniem a co za tym idzie manipulowanie wiadomości sms, a także kodami dostępu,

- pominięciu przez Sąd I instancji dowodu z dokumentu w postaci Raportu Komisji Nadzoru Finansowego „ Usługi (...) dla Klientów detalicznych- charakterystyka i zagrożenia", tezy ze str. 11 oraz 12, http://www.knf.gov.pl/I./Raport_B._(...).pdf.

b) art. 278 k.p.c. w zw. z 233 § 1 k.p.c. poprzez uznanie, wbrew treści opinii biegłego, że pełną odpowiedzialność za przeprowadzone w sprawie nieautoryzowane transakcje ponosi pozwany mimo, że z treści opinii wynika w sposób jednoznaczny, że sposób korzystania przez użytkownika z komputera był naganny.

3. naruszenie prawa materialnego tj.:

a) art. 46 ust. 1 ustawy o usługach płatniczych poprzez jego błędne zastosowanie i przyjęcie odpowiedzialności pozwanego za kwestionowane w niniejszym postępowaniu transakcje,

b) art. 46 ust. 3 ustawy o usługach płatniczych poprzez jego niezastosowanie i uznanie, że powodowie nie odpowiadają za transakcje nie doprowadziwszy do nich wskutek rażącego niedbalstwa,

c) art. 362 k.c. poprzez jego niezastosowanie, gdy z okoliczności sprawy wynika, że gdyby nie zaniechania oraz czynności podejmowane przez powodów w sprawie nie doszłoby do powstania szkody.

W konkluzji apelujący wniósł o uchylenie zaskarżonego wyroku oraz przekazanie sprawy do ponownego rozpoznania Sądowi I instancji, ewentualnie o zmianę przedmiotowego orzeczenia poprzez oddalenie powództwa w całości, a także o zasądzenie od powodów na rzecz pozwanego kosztów zastępstwa procesowego za I i II instancję według norm przepisanych.

W odpowiedzi na apelację powodowie wnieśli o oddalenie apelacji oraz o zasądzenie od pozwanego na rzecz każdego z powodów kosztów postępowania apelacyjnego, w tym kosztów zastępstwa procesowego według norm przepisanych.

Sąd Apelacyjny zważył co następuje:

Apelacja nie była uzasadniona.

Skuteczne podważenie wyroku sądu pierwszej instancji wymaga wskazania takich etapów stosowania przepisów prawa materialnego i procesowego, którym sąd uchybił. Konieczne jest w tym względzie nie tylko samo odniesienie się do konkretnych ustaleń i ocen prawnych jakie Sąd Okręgowy wyraził w swoim uzasadnieniu, ale również wykazanie podstawy prawnej, z którą te ustalenia lub oceny są sprzeczne. Powyższy obowiązek apelującego ma szczególne znaczenie w przypadku naruszenia norm prawa procesowego, w szczególności związanych z oceną materiału dowodowego zgromadzonego w aktach sprawy. Prawidłowość zastosowania lub wykładni prawa materialnego może bowiem być właściwie oceniona jedynie na kanwie niewadliwie ustalonej podstawy faktycznej rozstrzygnięcia. Ta zaś jest skutkiem oceny dowodów dokonanej przez sąd, polegającej na odmówieniu wiarygodności pewnym dowodom, a uznaniu innych za przekonujące.

Ocena wiarygodności i mocy dowodów jest podstawowym zadaniem sądu orzekającego, wyrażającym istotę sądzenia, a więc rozstrzygania kwestii spornych w warunkach niezawiłości, na podstawie własnego przekonania sędziego przy uwzględnieniu całokształtu zabranego materiału (wyrok SN z dnia 16 lutego 1996 r. II CRN 173/96, LEX nr 1635264). Skuteczne przedstawienie zarzutu naruszenia przez sąd art. 233 k.p.c. wymaga wykazania, że sąd uchybił zasadom logicznego rozumowania, lub doświadczenia życiowego, to bowiem jedynie może być przeciwstawione uprawnieniu sądu do dokonania swobodnej oceny dowodów. Nie jest natomiast wystarczające przekonanie strony o innej niż przyjął to sąd wadze poszczególnych dowodów i ich odmiennej ocenie niż ocena sądu (m. in. orzeczenie SN z dnia 10 stycznia 2002 r. r. II CKN 572/99, LEX nr 53136). Postawienie zarzutu obrazy art. 233 § 1 k.p.c. nie może polegać jedynie na zaprezentowaniu przez skarżącego stanu faktycznego przyjętego na podstawie własnej oceny dowodów, skarżący może tylko wskazywać, posługując się wyłącznie argumentami jurydycznymi, że sąd rażąco naruszył ustanowione w wymienionym przepisie zasady oceny wiarygodności i mocy dowodów oraz, że naruszenie to miało wpływ na wynik sprawy (m. in. wyrok SN z dnia 10 kwietnia 2000 r. V CKN 17/2000. OSNC 2000/10 poz. 189). Jeżeli więc z określonego materiału dowodowego sąd wyprowadza wnioski logicznie poprawne i zgodne z doświadczeniem życiowym, to ocena sądu nie narusza reguł swobodnej oceny dowodów i musi się ostać, chociażby w równym stopniu, na podstawie tego samego materiału dowodowego, dawały się wysnuć wnioski odmienne. Tylko w przypadku, gdy brak jest logiki w wiązaniu wniosków z zebranymi dowodami lub, gdy wnioskowanie sądu wykracza poza schematy logiki formalnej, albo wbrew zasadom doświadczenia życiowego nie uwzględnia związków przyczynowo – skutkowych, przeprowadzona przez sąd ocena dowodów może być skutecznie podważona (wyrok SN z dnia 27 września 2002 r. II CKN 817/00, LEX nr 56096).

W przedmiotowej sprawie powyższa sytuacja nie miała miejsca. Sąd Okręgowy, w wyniku prawidłowo przeprowadzonego postępowania dowodowego, uwzględniającego zasady rozkładu ciężaru dowodu (art. 6 k.p.c.) ustalił bowiem wszystkie okoliczności istotne dla rozstrzygnięcia sporu, które znajdowały odzwierciedlenie w

całokształcie zaoferowanego przez strony materiału dowodowego. Dokonując oceny tak zebranego materiału Sąd nie naruszył reguł swobodnej oceny dowodów, wyznaczonych treścią art. 233 k.p.c., a w szczególności zasad logiki, wiedzy i doświadczenia życiowego.

Wbrew wątpliwościom skarżącego, Sąd I instancji nie pominął wyjaśnień powodów na temat sposobu skorzystania przez L. S. z usługi bankowości elektronicznej pozwanego w dniu 4 lipca 2013 r. i dokonał w tej mierze ustaleń, które nie były sporne. Nie ulegał bowiem wątpliwości fakt, że tego dnia powód po rozpoczęciu procesu logowania uzyskał komunikat sugerujący zainstalowanie w telefonie komórkowym oprogramowania E- S. w celu poprawy jakości i bezpieczeństwa. Powód postąpił zgodnie z tą instrukcją i zainstalował żądaną aplikację podając w trakcie tego procesu numer telefonu. Umożliwiło to dokonanie przestępstwa polegającego na przelaniu znajdujących się na rachunkach oszczędnościowym środków pieniężnych na inne konta bez wiedzy i akceptacji powodów. Opisując przebieg powyższych czynności i charakter działania przestępców Sąd oparł się na opinii biegłego, która nie była kwestionowana przez żadną ze stron. Odnosząc się do tego ostatniego dowodu należało podkreślić, że dowód z opinii biegłego podlega ocenie sądu na podobnych zasadach jak inne dowody przeprowadzone w danej sprawie (art. 233 § 1 k.p.c.), przy czym nie można pomijać, że dowód ten nie jest dowodem subsydiarnym i podlega dopuszczeniu zawsze w sytuacji gdy dla rozstrzygnięcia sprawy konieczne są wiadomości specjalne (art. 278 k.p.c.). Przeprowadzenie dowodu z opinii biegłego było w niniejszej sprawie konieczne dla ustalenia z jakich przyczyn doszło do zainfekowania komputera należącego do powodów i niedozwolonego przelania pieniędzy. Tym niemniej ocena tego dowodu należała do Sądu I instancji który był władny nie tylko do uznania opinii za mniej lub bardziej miarodajną, ale również do uznania, że pewne tezy zawarte w opinii nie są przydatne dla rozstrzygnięcia sprawy. Ta ostatnia uwaga odnosiła się do tego fragmentu opinii, w której biegły wypowiedział się na temat naganności korzystania przez powoda z komputera przy wykonywaniu transakcji w dniu 4 lipca 2013 r. Ocena w tym zakresie należała do Sądu który dokonał jej w świetle całokształtu okoliczności sprawy.

Zarzucane w apelacji pominięcie dowodu z dokumentu w postaci Raportu (...) o tyle nie było zasadne, że strona pozwana nie wskazała na jakie konkretne okoliczności dowód ten miał być przeprowadzony, nie wyjaśniła ponadto, jaki wpływ brak ten miał na wynik przedmiotowego postępowania.

Nie można też było pominąć, że w większości argumenty przytoczone w apelacji nie tyle dotyczyły oceny dowodów ile miały związek z dokonaną przez Sąd I instancji subsumcją ustalonego stanu faktycznego do norm materialno prawnych o czym będzie mowa poniżej.

W podsumowaniu należało uznać, wbrew wywodom apelacji, że Sąd okręgowy nie dopuścił się naruszenia zarówno art. 233 § 1 k.p.c. jak i art. 278 k.p.c.

Chybione były też zarzuty odnoszące się do obrazy przytoczonych w apelacji przepisów prawa materialnego i nierozpoznania istoty sprawy.

Przesądzającą dla tej oceny była kwestia czy powodom można było przypisać postępowanie dowodzące zawinionego, w stopniu co najmniej rażącego niedbalstwa, udostępnienia danych umożliwiających dokonanie przedmiotowego przestępstwa.

Zgodnie z przytoczonymi przez Sąd przepisami ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, na dostawcy tych usług ciąży obowiązek zwrotu na rzecz płatnika kwoty transakcji w przypadku nieautoryzowanej transakcji płatniczej, z tym, że płatnik odpowiada za nieautoryzowaną transakcję w całości jeśli doprowadził do niej umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków o których mowa jest w art. 42 ustawy (art. 46 ust. 1). Obowiązki wymienione w art. 42 polegają na powinności korzystania z instrumentu płatniczego zgodnie z umową oraz konieczności niezwłocznego zgłaszania dostawcy utraty, kradzieży, przywłaszczenia lub nieuprawnionego użycia instrumentu płatniczego bądź nieuprawnego dostępu do tego instrumentu. Użytkownik jest też zobowiązany do podejmowania niezbędnych środków dla zapobiegania naruszaniu

indywidualnych zabezpieczeń tego instrumentu, a w szczególności jest zobowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym.

Nie można było przy tym pominąć, co zaakcentował Sąd Okręgowy, że ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub, że została wykonana prawidłowo spoczywa na dostawcy. Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez płatnika autoryzowana. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzowanie transakcji przez płatnika albo okoliczności wskazujących na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego obowiązków o których mowa jest a art. 42 ustawy (art. 42 ustawy)

Transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na jej wykonanie w sposób przewidziany umową (art. 40 ust. 1 ustawy).

W świetle ponownie przeanalizowanych okoliczności niniejszej sprawy, prawidłowo ustalonych przez Sąd I instancji, należało zgodzić się ze stanowiskiem, że powodom nie można było przypisać autoryzacji przedmiotowych transakcji płatniczych, strona pozwana nie wykazała również, a na niej spoczywał w tym względzie ciężar dowodu, by powodowie naruszyli zasady określone w art. 42 ustawy umyślnie bądź na skutek rażącego niedbalstwa.

Za tego rodzaju poglądem przemawiały argumenty przytoczone w uzasadnieniu zaskarżonego orzeczenia, dotyczące zwłaszcza charakteru dokonanego przestępstwa. Jak bowiem słusznie zaznaczył Sąd Okręgowy, powołując się w tym względzie na opinię biegłego, do zainfekowania komputera doszło w sposób podstępny, nie do przewidzenia dla przeciętnego użytkownika, nie posiadającego specjalistycznej wiedzy z zakresu informatyki. Przypomnieć należy, że po zalogowaniu, na tle strony internetowej Banku pojawił się nieusuwalny komunikat zawierający informację w sprawie dokonania czynności mającej na celu poprawę jakości i bezpieczeństwa usług. Żądanie to, wobec trudności z uzyskaniem połączenia, mogło się przedstawić jako wiarygodne. Tym samym obsługującemu komputer powodowi, który wykonał polecenie zwarte w komunikacie, nie można było przypisać rażącego niedbalstwa. Wymaga też podkreślenia, że w czasie kiedy doszło do przedmiotowego zdarzenia, bankowość elektroniczna nie była tak szeroko rozwinięta jak obecnie, nie były też powszechnie znane zagrożenia związane z tego rodzaju usługami. W tym okresie na stronie internetowej Banku z której korzystali powodowie nie było stosownych informacji i ostrzeżeń dotyczących podobnego schematu działania cyberprzestępców, zwłaszcza na temat programów które mogą zagrażać telefonom komórkowym. Zdarzenie jakie dotknęło powodów nie było odosobnione, inni użytkownicy również nie byli w stanie odróżnić fałszywej strony internetowej Banku od niezainfekowanej i doznali szkody na skutek tego samego przestępczego działania.

Powodowie nie informowali nikogo o swoim haśle ani loginie do konta, nie dokonywali przelewów z karty kredytowej, nie korzystali nadto z opcji zapamiętywania hasła dostępu do konta. Komputer powoda posiadał aktywne zabezpieczenie antywirusowe i włączoną zaporę systemową. Okoliczność, że system ten nie cechował się wysoką skutecznością nie miała znaczenia wobec braku, co trafnie podkreślił Sąd I instancji, szczególnych wymagań ze strony Banku co do sposobu zabezpieczenia komputera (rodzaju oprogramowania antywirusowego i stopnia jego skuteczności) w czasie zawierania umowy. Z podobnych względów należało ocenić jako nieskuteczny argument przywołujący stwierdzenie biegłego, iż sposób wykorzystywania systemu komputerowego przez użytkownika był naganny z punktu widzenia bezpieczeństwa systemów komputerowych gdyż komputer na którego dysku ściągane są pliki niewiadomego pochodzenia nie powinien być wykorzystywany do internetowych transakcji bankowych.

Jedynie w razie wykazania, czego apelujący nie uczynił, że powodowie uchybili umownym obowiązkom w powyższym zakresie można byłoby rozważyć to zaniechanie w kategoriach rażącego niedbalstwa.

Sąd Okręgowy nie bez racji zwrócił też uwagę na te aspekty działania pozwanego, które budziły zastrzeżenia co do jego profesjonalizmu. Stosownie do art. 50 ust. 2 ustawy prawo bankowe na bankach ciąży powinność dołożenia szczególnej staranności w zakresie prowadzenia rachunków bankowych oraz zapewnienia maksimum bezpieczeństwa dla wkładów pieniężnych i przeciwdziałania wypłaty tych środków na rzecz osób nieuprawnionych. Trudno było

uznać jako w pełni odpowiadające tym wymogom działanie polegające na braku odpowiedniej reakcji na dokonywane na kontach powodów operacje bankowe dotyczące przelewu w krótkim czasie znacznych kwot, odpowiadających praktycznie całości wkładów, w sytuacji gdy do momentu tych transakcji powodowie dokonywali jedynie drobnych płatności.

Mając na względzie treść art. 42 ust. 2 ustawy o usługach płatniczych, Sąd obniżył należną powodom kwotę o równowartość 150 euro, będącą swoistego rodzaju karą za naruszenie jednego obowiązków ciążących na mocy powyższej normy prawnej. Odpowiedzialność ta jest niezależna od winy płatnika i mogła być przypisana powodom niezależnie od tego, że omawianego naruszenia dopuścili się w sposób niezamierzony i nieświadomy.

Zdaniem Sądu Apelacyjnego, nie było natomiast podstaw do zastosowania w niniejszej sprawie art. 362 k.c. Uregulowana w tym przepisie instytucja nie miała zastosowania wobec przesądzenia, że powodowie nie dopuścili się innych nagannych działań niż te, które uprawniały do obciążenia ich równowartością 150 euro.

Ostatecznie, z podanych wyżej przyczyn, Sąd Apelacyjny oddalił apelację stosownie do treści art. 385 k.p.c. O kosztach postępowania odwoławczego Sąd ten rozstrzygnął w oparciu o art. 98 § 1 k.p.c. w zw. z art. 108 § 1 k.p.c. i art. 390 § 1k.p.c.