Sygn.akt III Ca 24/16

UZASADNIENIE

Zaskarżonym wyrokiem z dnia 28 września 2015 roku wydanym w sprawie o sygn.akt II C 383/15 z powództwa A. T. przeciwko Bankowi (...) Spółce Akcyjnej we W. Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi zasądził od pozwanego na rzecz powódki kwotę 18450,81 złotych z ustawowymi odsetkami od dnia 5 września 2014 roku do dnia zapłaty oraz kwotę 3053,88 złotych tytułem zwrotu kosztów procesu i oddalił powództwo w pozostałej części.

Sąd Rejonowy swoje rozstrzygnięcie oparł na następujących ustaleniach faktycznych:

na podstawie umowy ramowej rachunków z dnia 4 marca 2003 roku (...) Bank S.A. w W. (obecnie: Bank (...) S.A. we W.) prowadził dla powódki A. T. indywidualny rachunek oszczędnościowo - rozliczeniowy pod nazwą (...) nr (...). W dniu 28 listopada 2006 roku (...) Bank S.A. w W. otworzył na rzecz powódki w ramach umowy rachunku (...) z dnia 4 marca 2003 r. ponadto konto oszczędnościowe nr (...).

Powódka korzystała w pozwanym Banku z usług bankowości elektronicznej. Klientom pozwanego, którzy deklarują chęć korzystania z usług bankowości elektronicznej, nie są stawiane żadne wymagania sprzętowe ani dotyczące oprogramowania. Bank sugeruje jedynie, by klient korzystał z programu antywirusowego, aktualnego systemu operacyjnego i przeglądarki. W celu uzyskania dostępu do usług elektronicznych banku wystarczy standardowy komputer z popularnym systemem operacyjnym i jedną z pięciu najpopularniejszych przeglądarek. Dla uzyskania dostępu do konta drogą elektroniczną, klient pozwanego podaje dane identyfikacyjne z tzw. KB karty oraz (...) ustalony przez niego w oddziale Banku. Do autoryzacji transakcji płatniczych konieczne jest natomiast podanie ponadto żądanego hasła (numerów identyfikacyjnych) z listy haseł jednorazowych oraz powtórzenie znaków wyświetlonych na ekranie. Hasła z listy haseł jednorazowych nie są wykorzystywane w pozwanym Banku do identyfikacji klientów na etapie logowania, a jedynie do autoryzacji transakcji.

W pozwanym Banku powstają pliki systemowe z listami haseł jednorazowych, tworzone przez biblioteki kryptograficzne. Są one szyfrowane i wysyłane Państwowej Wytwórni Papierów Wartościowych, która drukuje listy i ich identyfikatory, a następnie przekazuje do Banku jako druki tajne w tzw. bezpiecznych kopertach. Pracownicy Banku nie mogą uzyskać dostępu do zawartości koperty. Są one zabezpieczone przez podejrzeniem, a ich naruszenie można stwierdzić „gołym okiem". Dostęp do haseł uzyskuje jedynie klient - posiadacz listy.

Powódka korzystała z narzędzia do autoryzacji transakcji internetowych w postaci haseł jednorazowych, które odbierała w oddziale Banku w formie papierowej. Listę przechowywała najczęściej w domu w szufladzie.

Pozwany Bank zamieszcza na swoich stronach internetowych ostrzeżenia przed podawaniem przez klientów danych umożliwiających dostęp do ich rachunków bankowych podmiotom innym niż bank, który prowadzi rachunek, przed nietypowymi ekranami żądającymi podania danych służących do autoryzacji dyspozycji (haseł z listy haseł jednorazowych lub tokena), niestandardowymi prośbami o podanie danych dotychczas niewymaganych na stronie logowania, jak hasła jednorazowe wykorzystywane wyłącznie do autoryzacji dyspozycji, przed złośliwym oprogramowaniem; zamieszcza także informacje wskazujące prawidłowy adres serwisu bankowości elektronicznej („https:/", a nie „http:/") i o konieczności pojawienia się symbolu zamkniętej kłódki w pasku adresowym przeglądarki, odsyła też do komunikatów Komisji Nadzoru Finansowego. 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. Ostrzeżenia tego typu pojawiały się na stronie internetowej Banku także przed 22 maja 2014 roku. Niektóre ostrzeżenia wymagają potwierdzenia, że klient zapoznał się z nimi. Nie jest jednak wykluczone potwierdzenie tej informacji przez cyberprzestępców.

Pozwany Bank posiada specjalne mechanizmy, które sprawdzają zawartość przeglądarki internetowej po stronie klienta pod kątem obecności złośliwego oprogramowania. Pozwany wymienia informacje na temat przestępczości w sieci z innymi bankami, instytucjami, firmami zewnętrznymi. Bank otrzymał sygnał od firmy zajmującej się

bezpieczeństwem w cyberprzestrzeni, że w dniach 22 -23 maja 2014 roku pojawiła się nowa konfiguracja złośliwego oprogramowania.

W dniu 22 maja 2014 roku powódka dziewięciokrotnie, a w dniu 23 maja 2014 roku - jednokrotnie, bezskutecznie próbowała logować się, by uzyskać dostęp do swoich rachunków w pozwanym Banku za pośrednictwem Internetu. W dniu 23 maja 2014 r. o godzinie 12:05:41 w serwisie powódki pozwany wyświetlił nowy komunikat bezpieczeństwa dotyczący zagrożenia w sieci. Gdy powódka logowała się do konta w dniu 23 maja 2014 r. nie widziała żadnych ostrzeżeń.

Na stronie, która wyświetlała się po wpisaniu adresu strony internetowej Banku, powódka podawała login i hasło (dane z KB Karty i (...)), lecz strona zawieszała się, a po pewnym czasie ukazywała się informacja, że nie można uzyskać połączenia z Bankiem. Na żądanie wyświetlone na stronie internetowej powódka przynajmniej dwukrotnie podała też hasło z listy haseł jednorazowych, będącej w jej posiadaniu, jednak w dniach 22 i 23 maja 2014 roku nie uzyskała dostępu do rachunków i nie dokonywała na nich żadnych operacji. W dniu 22 maja 2014 roku o godzinie 10:43:50 rachunek oszczędnościowy powódki nr (...) został obciążony na rzecz posiadacza rachunku o numerze (...) 0000 0001 2340 (...), posługującego się nazwiskiem V. A., kwotą 9.800 zł.

W dniu 23 maja 2014 r. o godzinie 12:09:00 rachunek oszczędnościowy powódki nr (...) został obciążony na rzecz posiadacza rachunku o numerze (...) 0000 0001 2338 8510, posługującego się nazwiskiem A. T. kwotą 9.900 zł.

Pieniądze z konta powódki zostały przelane na konta otwarte w pozwanym Banku około dwóch tygodni wcześniej, a następnie - w ciągu kilku godzin od wykonania przelewów - wypłacone w placówkach pozwanego Banku w W. i B..

Treść i wygląd strony internetowej, jaka wyświetliła się powódce w dniach 22 - 23 maja 2014 roku, jest nie do ustalenia.

W dniu 27 maja 2014 roku powódce udało się zalogować do konta. Stwierdziła wówczas, że z jej rachunku oszczędnościowego, bez jej wiedzy i zgody, wykonano opisane wyżej przelewy na rzecz nieznanych jej beneficjentów. W tym samym dniu powódka zgłosiła osobiście reklamację w oddziale pozwanego Banku w Ł.. Konta powódki oraz dostęp do usług bankowości elektronicznej zostały zablokowane, a lista haseł jednorazowych unieważniona. Tego samego dnia powódka zgłosiła również sprawę Policji.

Przed dniem 22 - 23 maja 2014 roku powódka nie otrzymała żadnych wiadomości pocztą elektroniczną dotyczących konta, nie przekazywała innym osobom danych z nim związanych. Na komputerze, z którego powódka próbowała logować się w dniach 22 - 23 maja 2014 roku, znajdującym się w jej miejscu pracy, nie korzystała z opcji zapamiętywania hasła dostępu do konta.

W maju 2014 roku pojawiły się również inne przypadki zniknięcia pieniędzy z kont klientów pozwanego banku wskutek przelewów wykonanych z wykorzystaniem haseł z list haseł jednorazowych, znajdujących się w posiadaniu tych klientów. W przeglądarce klienta wyświetlała się strona przypominająca wyglądem stronę internetową Banku, na której pojawiały się prośby o podanie danych identyfikacyjnych do logowania oraz kodu z listy haseł jednorazowych. W maju 2014 roku nie doszło do złamania systemu informatycznego zabezpieczeń Banku, lecz do złamania zabezpieczeń po stronie przeglądarek, z których korzystali klienci.

C., na drugim komputerze przeprowadzał operacje na koncie klienta Banku z wykorzystaniem danych zbieranych przez złośliwe oprogramowanie zainstalowane na komputerze klienta: loginu, hasła, kodu z listy haseł jednorazowych wpisanego przez klienta na podstawionej stronie internetowej. Strona podstawiona posiada z reguły jak najwięcej oryginalnych elementów, mogą na niej również pozostać ostrzeżenia, by uwiarygodnić jej wygląd. Do zainstalowania złośliwego oprogramowania na komputerze klienta dochodzi np. wskutek kliknięcia w wyświetlone na stronie internetowej zdjęcie, za pośrednictwem plików przesyłanych pocztą elektroniczną, przez otwarcie zainfekowanego załącznika np. rzekomej faktury czy zestawienia nierozliczonych płatności.

Pismem z 5 września 2014 roku pozwany poinformował powódkę o wynikach przeprowadzonych przez Bank analiz dotyczących przyczyn zaistniałej sytuacji, wskazując, że nie można wykluczyć działania złośliwego oprogramowania na komputerze, który był narzędziem do złożenia kwestionowanych przez powódkę dyspozycji, pozostawiając dalsze czynności wyjaśniające organom ścigania.

Postanowieniem z dnia 28 listopada 2014 roku umorzono dochodzenie w sprawie podejrzenia popełnienia przestępstwa, polegającego na bezprawnym wpłynięciu na automatyczne przetwarzanie i przekazywanie danych informatycznych związanych z prowadzeniem przez Bank (...) S.A. rachunku oszczędnościowego o nr (...) prowadzonego dla A. T. i włamania po przełamaniu elektronicznych zabezpieczeń tego rachunku, z którego następnie dokonano kradzieży pieniędzy w łącznej kwocie 19.700 zł na szkodę (...) S.A. — wobec niewykrycia sprawcy przestępstwa.

Pismem z 12 grudnia 2014 roku pozwany podtrzymał stanowisko zajęte w piśmie z 5 września 2014 roku, odmawiając uznania roszczeń powódki.

Pismem z 29 stycznia 2015 roku powódka wezwała pozwanego do zapłaty kwoty 19.700 zł. Bank odmówił zwrotu środków.

Zgodnie z „Regulaminem kont dla ludności", obowiązującym w pozwanym Banku i stanowiącym integralną część umowy ramowej rachunków, w przypadku wystąpienia transakcji płatniczej nieautoryzowanej Bank powinien niezwłocznie zwrócić posiadaczowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku, gdy posiadacz korzystał z rachunku płatniczego, przywrócić obciążony rachunek do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Sąd Rejonowy powyższy stan faktyczny ustalił na podstawie zeznań powódki, świadków oraz dokumentów, których treść nie była kwestionowana przez żadną ze stron. Sąd pierwszej instancji oddalił wniosek o dopuszczenie dowodu z opinii biegłego z zakresu informatyki ze znajomością problematyki bezpieczeństwa bankowych systemów informatycznych i ich zawartości, przestępczości internetowej, wyszukiwania, odzyskiwania i analizy danych świadczących o aktywności użytkowników komputera oraz bankowości - na okoliczności sprecyzowane w odpowiedzi na pozew. W ocenie Sądu dowód ten nie przyczyniłby się do wyjaśnienia okoliczności istotnych dla rozstrzygnięcia sprawy i był częściowo nieadekwatny dla osiągnięcia założonego celu. Zmierzał bowiem w znacznej mierze do ustalenia faktów, nie zaś ich analizy w świetle wiadomości specjalnych. Pytania, o których postawienie biegłemu wnosił pozwany, miały charakter pytań natury ogólnej, bez bezpośredniego związku z rozpoznawaną sprawą. Ponadto, decydujące dla wyniku procesu było ustalenie przede wszystkim działań powódki i ich ocena z punktu widzenia określonego miernika staranności. Rodzaj stosowanych przez Bank zabezpieczeń informatycznych miał natomiast znaczenie drugoplanowe i został w przekonaniu sądu orzekającego w dostatecznym stopniu wykazany za pomocą zeznań świadków strony pozwanej.

Przy tak ustalonym stanie faktycznym Sąd Rejonowy uznał, że roszczenie powódki znajduje oparcie w przepisach ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (t. jedn. Dz. U. z 2014 r., poz. 873 ze zmianami),określającej między innymi prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych, a także zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych (art. 1 pkt 2 ustawy).

Sąd pierwszej instancji wskazał, iż 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 powódce zaś - jako użytkowniku instrumentu płatniczego - spoczywał obowiązek korzystania z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu (art. 42 ust. 1 pkt 1 i 2). W celu spełnienia powyższego obowiązku użytkownik, z chwilą otrzymania instrumentu płatniczego, winien podejmować niezbędne środki zapobiegające naruszeniu indywidualnych zabezpieczeń instrumentu, w szczególności jest obowiązany do

przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (art. 42 ust. 2).

W ocenie Sądu pozwany Bank wywiązywał się z obowiązku zapewnienia,że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, powódka natomiast swoim obowiązkom wymienionym w art. 42 ust. 2 ustawy uchybiła, udostępniając instrument płatniczy osobom nieuprawnionym przez wpisanie przynajmniej dwukrotnie w dniach 22 i 23 maja 2014 r. kodów z listy haseł jednorazowych na podstawionej stronie internetowej. Udostępnienie przez powódkę danych identyfikacyjnych oraz haseł z listy będącej w jej posiadaniu osobom nieuprawnionym o nieustalonej tożsamości umożliwiło tym osobom zalogowanie się do jej konta i wykonanie dwóch przelewów. Czynności te z punktu widzenia systemu informatycznego Banku były przeprowadzone poprawnie, przy wykorzystaniu właściwych narzędzi autoryzacyjnych. Mimo tego, kwestionowanych transakcji płatniczych wykonanych z konta powódki w dniach 22 i 23 maja 2014 roku nie można uznać – w ocenie Sądu, za transakcje autoryzowane. Zgodnie z art. 40 ust. 1 powołanej wyżej ustawy transakcję uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji w sposób przewidziany w umowie między płatnikiem a jego dostawcą. W świetle poczynionych w sprawie ustaleń nie ulega wątpliwości,że powódka takiej zgody nie wyraziła. Świadczy o tym również fakt, że niezwłocznie powiadomiła pozwanego oraz Policję, stosownie do obowiązków wynikających z art. 44 ust. 1 przywoływanej ustawy, celem wyjaśnienia przyczyn zniknięcia z konta niemal całych posiadanych przez nią oszczędności.

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

Sąd Rejonowy podniósł, że w okolicznościach niniejszej sprawy nie można powódce przypisać zgody ani woli podjęcia czynności zmierzających do przeprowadzenia kwestionowanych transakcji płatniczych przy użyciu posiadanych przez nią instrumentów płatniczych, a które to okoliczności świadczyłyby o autoryzowaniu przez nią transakcji. Nie można jej również przypisać umyślnego doprowadzenia do nieautoryzowanych transakcji płatniczych, choćby z tej przyczyny, że o ich dokonaniu powódka dowiedziała się dopiero w dniu 27 maja 2014 roku. Zostały one zatem przeprowadzone bez jej wiedzy. W ocenie Sądu pierwszej instancji, nie można powódce również przypisać rażącego niedbalstwa w naruszeniu obowiązków, wynikających z art. 42 ustawy. Wprawdzie powódka udostępniła osobom nieuprawnionym dane z listy haseł jednorazowych, czego nie powinna czynić, jednak nie nastąpiło to w okolicznościach świadczących o rażącym niedbalstwie z jej strony. Jak wynika ze zgromadzonego w sprawie materiału dowodowego, do zainfekowania komputera użytkownika usług bankowości elektronicznej może dojść w podstępny, lecz prosty sposób, np. przez kliknięcie przez użytkownika w zdjęcie na ekranie czy otwarcie załącznika do wiadomości nadesłanej pocztą elektroniczną, informującej np. o nierozliczonych płatnościach czy zawierającej rzekome faktury. Powódka w okresie poprzedzającym kwestionowane transakcje nie otrzymała żadnej wiadomości dotyczącej bezpośrednio jej kont w pozwanym Banku ani nie przekazywała pocztą elektroniczną informacji ich dotyczących. Powódka nie udostępniła nikomu swojej listy haseł jednorazowych w formie papierowej ani jej nie zagubiła. W dniach 22 i 23 maja 2014 roku korzystała z komputera w swoim miejscu pracy, jak twierdzi, a czemu pozwany nie zaprzeczył - z legalnym oprogramowaniem i zabezpieczonego programem antywirusowym, choć Bank nie stawiał swoim klientom niemal żadnych wymagań dotyczących sprzętu i oprogramowania. W komputerze użytym przez powódkę login i hasło dostępu do konta nie były zapamiętane ani podpowiadane. Po wprowadzeniu do komputera adresu strony internetowej Banku wyświetliła się witryna imitująca stronę Banku, o treści i wyglądzie dziś już niemożliwym do odtworzenia, na której żądano podania przez powódkę zwyczajowych danych do logowania (identyfikatora z KB Karty i (...)u) oraz dodatkowego uwierzytelnienia swojej tożsamości przez wpisanie kodu z listy haseł jednorazowych. Żądanie to, wobec trudności z uzyskaniem połączenia, mogło przedstawiać się wiarygodnie. Jak zeznawali świadkowie, na stronach podstawionych hackerzy pozostawiają jak najwięcej elementów oryginalnych, niekiedy również ostrzeżenia przed zagrożeniami w sieci, aby uwierzytelnić ich wygląd. Wprawdzie świadek M. K. (1) zeznała, że strony takie cechuje często nieporadność językowa i stylistyczna, brak jednak dowodów, by z taką właśnie

niepoprawnie zredagowaną stroną zetknęła się powódka. Bezspornym jest, że w maju 2014 roku nie tylko powódka padła ofiarą ataku cyberprzestępców, lecz także kilkunastu innych klientów pozwanego Banku. Przemawia to za tym, że strona nie przedstawiała się jako oczywiście fałszywa. Jak wynika z ustaleń, komunikat dotyczący tego zagrożenia, z którym zetknęła się powódka, został skierowany bezpośrednio do niej i do klientów Banku już po zrealizowaniu przez Bank obu spornych przelewów, tj. w dniu 23 maja2014 r. po godz. 12.00. Wprawdzie na stronach Banku zamieszczano ostrzeżenia przed podawaniem dodatkowych danych identyfikacyjnych także przed 22 maja 2014 roku, jednak to właśnie na stronie Banku (a w rzeczywistości na stronie ją imitującej), a nie w innym miejscu i okolicznościach, zażądano od powódki podania konkretnego hasła z wydanej jej przez Bank listy haseł jednorazowych. W ocenie Sądu, powyższe okoliczności, nie pozwalają na przypisanie powódce rażącego niedbalstwa w związku z wpisaniem na stronie internetowej imitującej stronę Banku kodów służących co do zasady do autoryzacji transakcji, a nie do weryfikacji tożsamości. Sąd Rejonowy wskazał,że zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych oraz postanowieniami regulaminu stanowiącego integralną część łączącej strony umowy rachunku bankowego, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

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

Mając na uwadze powyższe Sąd Rejonowy zasądził na rzecz powódki kwotę 18.450.81 zł, pomniejszając żądane przez powódkę 19.700 zł zgodnie z dyspozycją art. 46 ust. 2 ustawy w następujący sposób:

- 9.800 zł przelane z konta w dniu 22 maja 2014 r. o 626,33 zł, odpowiadające równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego 4, (...), ogłaszanego przez NBP i obowiązującego w dniu wykonania tej transakcji (Tabela nr (...) z dnia 22 maja 2014 r.),

9.700 zł przelane z konta w dniu 23 maja 2014 r. o 622,86 zł, odpowiadające równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego 4, (...), ogłaszanego przez NBP i obowiązującego w dniu wykonania tej transakcji (Tabela nr (...) z dnia 23 maja 2014 r.). W zakresie kwoty 1249,19 zł (626.33 zł + 622,86 zł) żądanej tytułem należności głównej powództwo podlegało oddaleniu.

Ponieważ pozwany dopuścił się opóźnienia w zwrocie zasądzonej wyrokiem kwoty, powódce należały się odsetki w wysokości ustawowej zgodnie z art. 481 § 1 i 2 k.c. od dnia 5 września 2014 r. (do dnia zapłaty). W tej dacie Bank wystosował do powódki odpowiedź na reklamację, informując o poczynionych we własnym zakresie ustaleniach. Wówczas pozwany niewątpliwie posiadał już wiedzę o okolicznościach niezbędnych dla ustalenia własnej odpowiedzialności. Odmawiając powódce zwrotu środków pieniężnych, popadł z tą chwilą w opóźnienie. Żądanie odsetek w dalej idącym zakresie podlegało oddaleniu.

O kosztach postępowania Sąd Rejonowy orzekł w oparciu o art. 100 k.p.c. zgodnie z zasadą stosunkowego ich rozdzielenia przyjmując, iż powódka wygrała proces w 94%.

Apelację od opisanego wyżej orzeczenia wniósł pozwany zaskarżając wyrok w całości i zarzucając Sądowi Rejonowemu:

1.naruszenie art. 233 § 1 k.p.c. poprzez błędną ocenę zebranego w sprawie materiału dowodowego i w konsekwencji:

- błąd w ustaleniach faktycznych polegający na przyjęciu, że pozwany posiada specjalne mechanizmy, które sprawdzają zawartość przeglądarki internetowej po stronie klienta pod kątem obecności złośliwego oprogramowania. Tymczasem po pierwsze taki mechanizm jest powszechnie dostępny, a po drugie, zawartość przeglądarki internetowej możliwa jest do sprawdzenia jedynie na komputerze, z którego logowano się do usług bankowości elektronicznej tj.na którym doszło do zainstalowania wirusa,

- błąd w ustaleniach faktycznych polegający na przyjęciu, że powódka, gdy logowała się do konta w dniu 23 maja 2014 roku nie widziała żadnych ostrzeżeń, choć ostrzeżenia takie pojawiały się na stronie do logowania do usług bankowości elektronicznej pozwanego co najmniej od początku maja 2014 roku.Ponadto Sąd Rejonowy całkowicie pominął fakt, że powódka pomimo tego, że 22 maja 2014 roku wprowadziła hasło autoryzujące, to dodatkowo uczyniła to dzień później przyczyniając się do większej szkody,

- błąd w ustaleniach faktycznych i w konsekwencji przyjęcie, że treść i wygląd strony internetowej, jaka wyświetliła się powódce w dniach 22-23 maja 2014 roku jest nie do ustalenia. Taki wniosek jest sprzeczny z tym, co zeznali świadkowie powołani przez pozwanego. Dodatkowo, na okoliczność tę powołany był przez pozwanego dowód z opinii biegłego, który Sąd I instancji pominął (oddalił),

- błąd w ustaleniach faktycznych polegający na przyjęciu, iż powódka udostępniła instrument płatniczy osobom nieuprawnionym przez podanie im danych do logowania i autoryzacji transakcji w sposób niezamierzony i nieświadomy, a tym samym jej działaniom nie można przypisać rażącego niedbalstwa;

2)naruszenie 217 § 1 w zw. z art. 227 k.p.c. poprzez pominięcie dowodu z opinii biegłego i błędne uznanie, że okoliczności sporne zostały już dostatecznie wyjaśnione, a ponadto, że okoliczności sprecyzowane przez pozwanego w odpowiedzi na pozew nie przyczyniłyby się do wyjaśnienia okoliczności istotnych dla rozstrzygnięcia sprawy.

W ocenie pozwanego, sąd I instancji przekroczył granice swobodnej oceny dowodów, albowiem dopuścił się błędów logicznego rozumowania, ocenił dowody sprzecznie z doświadczeniem życiowym, zasadami logicznego rozumowania i bez ich wszechstronnego rozważenia. Jak wskazał pozwany, zeznania świadków - B. T., M. P. (1) i M. K. (1) jednoznacznie potwierdziły, że mechanizmy sprawdzające zawartość przeglądarki internetowej klienta dostępne są powszechnie, a nie - jak błędnie przyjął Sąd - przez pozwanego. Dodatkowo Sąd całkowicie pominął fakt, że takim narzędziem owszem dysponuje pozwany, jednak można je wykorzystać „po fakcie", a więc po otrzymaniu informacji przez Bank (pozwanego) o ewentualnym wirusie, na dodatek bezwzględnie wymaga komputera, z którego nastąpiło logowanie do usług bankowości elektronicznej, tj. na którym doszło do zainstalowania złośliwego oprogramowania.

Jak wynika z zeznań wszystkich świadków strony pozwanej, ostrzeżenia o pojawiających się w sieci Internet wirusach i to takich, z którym mamy do czynienia w niniejszej sprawie, pojawiały się na stronie do logowania do usług bankowości elektronicznej pozwanego co najmniej od początku maja 2014 r. Powódka zatem mogła i powinna się z nimi zapoznać, a co więcej respektować je. Ponadto, Sąd I instancji całkowicie pomiął fakt, że powódka pomimo tego, że 22 maja 2014 r. wprowadziła hasło autoryzujące i to nie do zaakceptowania transakcji, pomimo tego, że okoliczności wpisywania hasła były inne niż dotychczas, to dodatkowo uczyniła to dzień później, doprowadzając do powstania szkody w tak znacznej wysokości.

Według pozwanego wygląd strony internetowej, jaka wyświetliła się powódce w dniach 22-23 maja 2014 roku jest do ustalenia z dużą dozą prawdopodobieństwa. Jej wygląd opisali świadkowie, a co więcej pomógłby go ustalić biegły, albowiem posiada on wiadomości z zakresu wiedzy specjalnej. Sąd jednak oddalił ów wniosek dowodowy pozwanego.

Pozwany nie zgodził się przede wszystkim z przyjętą przez Sąd I instancji tezą, iż powódka udostępniła instrument płatniczy (dane do logowania do usług bankowości elektronicznej i autoryzacji transakcji) osobom nieuprawnionym poprzez podanie im danych do logowania i autoryzacji transakcji w sposób niezamierzony i nieświadomy, a tym samym jej działaniom nie można przypisać rażącego niedbalstwa. W ocenie pozwanego, to powódka ponosi

odpowiedzialność za sporne transakcje płatnicze na podstawie art. 46 ust. 3 UUP, albowiem doprowadziła do nich wskutek naruszenia, będącego skutkiem rażącego niedbalstwa, obowiązków, o których mowa w art. 42 UUP. Świadomie, wbrew postanowieniom umownym, naruszyła poufność narzędzi wykorzystywanych w usługach (...), a tym samym bezpieczeństwo środków pieniężnych zgromadzonych na rachunkach powoda, gdyż udostępniła dane do logowania i autoryzacji osobom trzecim, dwukrotnie i to pomimo tego, że na stronach do logowania do usług bankowości elektronicznej pozwanego pojawiały się komunikaty ostrzegające przed tego typu wymuszeniami. Zdaniem pozwanego, sprawa nie została w tym zakresie dostatecznie wyjaśniona, zaś biegły wyjaśniłby szereg wątpliwych kwestii, w szczególności co do wyglądu strony jaka pojawiła się powódce celem wyłudzenia od niej danych do logowania i autoryzacji dyspozycji. Sąd oddalił dowód z opinii biegłego chociaż został powołany już w odpowiedzi na pozew.

W konkluzji pozwany wniósł o zmianę zaskarżonego wyroku poprzez oddalenie powództwa w całości, ewentualnie o uchylenie wyroku i przekazanie sprawy Sądowi I instancji do ponownego rozpoznania oraz o zasądzenie od powoda na rzecz pozwanego kosztów procesu, w tym kosztów zastępstwa procesowego w obu instancjach.

W odpowiedzi na apelację strona powodowa wniosła o jej oddalenie i zasądzenie kosztów postępowania odwoławczego.

Sąd Okręgowy zważył, co następuje:

Apelacja nie jest uzasadniona i dlatego podlega oddaleniu

W pierwszej kolejności należy zaznaczyć, że Sąd Okręgowy w pełni podziela prawidłowe ustalenia faktyczne poczynione przez Sąd Rejonowy uznając je za własne.

Podniesione w apelacji zarzuty naruszenia art. 233§1k.p.c. są bezpodstawne. W ocenie Sądu Okręgowego, Sąd Rejonowy dokonał oceny materiału dowodowego zgromadzonego w sprawie zgodnie z regułami ustanowionymi w powołanym przepisie.

Z utrwalonego już orzecznictwa Sądu Najwyższego wynika, iż skuteczne postawienie zarzutu naruszenia powołanego przepisu przez sąd wymaga wykazania, że sąd pierwszej instancji uchybił zasadom logicznego rozumowania lub doświadczenia życiowego, to bowiem jedynie może być przeciwstawione uprawnieniu sądu do dokonywania swobodnej oceny dowodów. Nie jest natomiast wystarczające przekonanie strony o innej niż przyjął sąd wadze poszczególnych dowodów i ich odmiennej ocenie niż ocena sądu (por.uzasadnienie wyroku Sądu Najwyższego z dnia 8 kwietnia 2009 roku II PK 261/08). Skarżący podnosząc tego rodzaju argument winien zatem wskazać konkretne zasady lub przepisy, które naruszył sąd przy ocenie określonych dowodów,czego skarżący w rozpoznawanej sprawie nie uczynił stawiając Sądowi Rejonowemu jedynie bardzo ogólnie sprecyzowane zarzuty.

W szczególności nie jest uzasadniony zarzut błędu w ustaleniach faktycznych polegającego na przyjęciu, że pozwany posiada specjalne mechanizmy sprawdzające zawartość przeglądarki internetowej klienta pod kątem obecności złośliwego oprogramowania. Powyższe ustalenie poczynione zostało na podstawie zeznań świadka strony pozwanej B. T., który podczas swoich zeznań złożonych na rozprawie w dniu 15 czerwca 2015 roku wyjaśniał, jakie zabezpieczenia stosowane są w pozwanym Banku. Świadek ten między innymi wskazał na istnienie kwestionowanych w apelacji mechanizmów, choć nie wyjaśnił dokładnie, w jaki sposób mogą zostać zastosowane. Trudno zatem przypisać Sądowi Rejonowemu błąd w ustaleniach faktycznych, skoro zostały poczynione zgodnie z treścią zeznań świadka. Należy także podkreślić, iż istnienie tego rodzaju mechanizmów bądź ich brak w rozpoznawanej sprawie nie miał większego znaczenia. Zainstalowanie złośliwego oprogramowania w przeglądarce internetowej powódki, które umożliwiło dokonanie przelewów z konta powódki przez osoby nieuprawnione, nie było kwestionowane i zostało przez Sąd uznane za udowodnione przede wszystkim na podstawie zeznań świadków strony pozwanej. Podstawą przyjęcia odpowiedzialności pozwanego był jednak brak autoryzacji transakcji, a nie niewłaściwa kontrola przeglądarki internetowej, z której korzystała powódka co do ewentualnego zabezpieczenia przed złośliwym oprogramowaniem.

Nie można także podzielić poglądu strony pozwanej, że Sąd Rejonowy popełnił błąd przyjmując, iż powódka nie widziała ostrzeżeń o wirusach komputerowych, choć Bank podobne ostrzeżenia zamieszczał na swoich stronach od początku maja 2014 roku. Przede wszystkim należy zauważyć, iż z zeznań świadka B. T. wynika, że w dniach 22-23 maja 2014 roku pojawiła się nowa konfiguracja złośliwego oprogramowania, co do której ostrzeżenia zostały zamieszczone po tej dacie. Świadek M. P. (2) wskazał z kolei, że klient otwierający stronę „zawirusowaną", nie widzi ostrzeżeń bankowych. Taka strona może zawierać „elementy wstrzykniętego kodu złośliwego, może być zmieniona". Potwierdzenie zapoznania się z wiadomością zawierającą ostrzeżenie może zostać przesłane z innego komputera niż komputer klienta banku.

Podkreślić należy również, iż świadkowie strony pozwanej – wbrew twierdzeniom zawartym w apelacji, nie opisali wyglądu strony internetowej, która wyświetliła się powódce. Przeciwnie – z zeznań świadka M. K. (1) wynika, że nie można z cała pewnością stwierdzić, jak wyglądała ta strona, ale jedynie można przypuszczać, jak mogła wyglądać i jakie komunikaty zawierać. Świadek B. T. wskazał nadto, iż przestępcy pozostawiają jak najwięcej oryginalnych elementów, aby uwiarygodnić wygląd strony.

Bezpodstawny jest także zarzut błędu w ustaleniach faktycznych polegającego na przyjęciu, iż powódka udostępniła kody jednorazowe w sposób niezamierzony i nieświadomy, a tym samym nie można powódce przypisać rażącego niedbalstwa . Skarżący formułując ten zarzut nie sprecyzował na czym miałby polegać błąd w ustaleniu faktów i na jakiej podstawie należałoby przyjąć,że powódka całkowicie świadomie przekazała kody jednorazowe nieuprawnionym podmiotom. Analiza uzasadnienia apelacji prowadzi do wniosku,że skarżący w istocie nie tyle na kwestionuje ustalenia faktyczne Sądu, lecz nieprawidłową – według pozwanego, ocenę prawną stanu faktycznego w tym zakresie. Fakt, iż powódka udostępniła kody jednorazowe osobom nieuprawnionym nie był kwestionowany przez stronę powodową i został prawidłowo ustalony przez Sąd – głównie na podstawie zeznań świadków strony pozwanej i przedstawionych przez te osoby wyników postępowania bankowego prowadzonego po zgłoszeniu powódki. Sporna była natomiast ocena prawna tego zdarzenia i to, czy działanie powódki należy ocenić jako rażące niedbalstwo, czy też – jak to uczynił Sąd Rejonowy, przypisać jej łagodniejszą postać winy.

Prawidłowe skonstruowanie zarzutów apelacji wymaga odróżnienia sytuacji, gdy w sprawie wadliwie ustalono stan faktyczny , czego konsekwencją był błędny proces subsumcji od sytuacji, w której prawidłowo ustalony stan faktyczny oceniono w świetle niewłaściwej normy prawnej. W pierwszym przypadku konieczne jest podniesienie zarzutów natury procesowej zmierzających do wykazania błędnego ustalenia przez sąd stanu faktycznego, a dopiero następnie zarzutów naruszenia prawa materialnego. W orzecznictwie Sądu Najwyższego wyrażany jest pogląd, że ani błędu w subsumcji nie można skutecznie dowodzić przez kwestionowanie prawidłowości dokonanych przez sąd ustaleń faktycznych, ani też zwalczanie prawidłowości ustaleń faktycznych nie może się odbywać za pomocą samego tylko zarzutu naruszenia prawa materialnego (wyroki Sądu Najwyższego: z 20 grudnia 2001 r. V CKN 510/00, Lex nr 53098; z 26 września 2002 r., III CKN 466/00, Lex nr 74408; z 19 kwietnia 2006 r., (...), Lex nr 198529, z 21 października 2004 r., V CK 81/04, Lex nr 146340; z 21 listopada 2008 r., V CSK 213/08, Lex nr 558628).

W ocenie Sądu Okręgowego, Sąd pierwszej instancji szczegółowo przeanalizował stan faktyczny i prawidłowo ocenił, iż powódka udostępniła kody jednorazowe i inne dane w sposób niezamierzony i nieświadomy. Powódka w swoim przekonaniu korzystała ze strony banku i działała w zaufaniu do wyświetlanych tam poleceń. Nie ulega wątpliwości, iż padła ofiarą przestępstwa i nie miała woli przekazania swoich oszczędności osobom, które dokonały wypłat z rachunków, na które przelano pieniądze. Bezsporną okolicznością jest to, iż w tym okresie pojawiło się więcej przypadków dokonania operacji z użyciem kodów jednorazowych, a zatem powódka nie była jedyną osobą, która nie zdołała się zorientować, iż korzysta z „zawirusowanej" strony internetowej. Powódka wcześniej korzystała wielokrotnie z usług bankowości elektronicznej, prawidłowo wykonując operacje i stosując się do wymagań banku. Pojawiające się w dniu 22 maja 2014 roku kłopoty z połączeniem z bankiem i komunikaty sugerujące konieczność dodatkowego „potwierdzenia" tożsamości klienta przez podanie kodu jednorazowego w połączeniu z wyglądem strony internetowej usprawiedliwiały przekonanie powódki o działaniu zgodnym z poleceniami banku.

Sąd Rejonowy dokonał zatem prawidłowych ustaleń faktycznych i w konsekwencji zasadnie ocenił, że powódce nie można przypisać rażącego niedbalstwa, choć nie ulega wątpliwości, że nie powinna udostępniać kodów jednorazowych do innych operacji niż autoryzacja transakcji.

Należy przy tym podkreślić, iż rażące niedbalstwo (culpa lata) jest kwalifikowaną postacią winy nieumyślnej. Oznacza zatem wyższy jej stopień niż w przypadku zwykłego niedbalstwa, leżący już bardzo blisko winy umyślnej (culpa lata dolo aequiparatur). Sąd Najwyższy w wyroku z dnia 25 września 2002 r., I CKN 969/00 (niepubl.) wskazał, że wykładnia pojęcia rażącego niedbalstwa powinna uwzględniać kwalifikowaną postać braku zwykłej staranności w przewidywaniu skutków. Konieczne jest zatem stwierdzenie, że podmiot, któremu taką postać winy chce się przypisać, zaniedbał takiej czynności zachowującej chronione dobro przed zajściem zdarzenia powodującego szkodę, której niedopełnienie byłoby czymś absolutnie oczywistym w świetle doświadczenia życiowego dostępnego każdemu przeciętnemu uczestnikowi obrotu prawnego i w sposób wprost dla każdego przewidywalny mogło doprowadzić do powstania szkody. Rażące niedbalstwo zachodzi bowiem tylko wtedy, gdy stopień naganności postępowania drastycznie odbiega od modelu właściwego w danych warunkach zachowania się dłużnika (wyrok SN z 22.04.2004 r., II CK 142/03, niepubl.).

O takim rażącym niedbalstwie można by mówić, gdyby powódka całkowicie świadomie udostępniła kody jednorazowe innej osobie, bądź przechowywała dane umożliwiające dostęp do jej konta w sposób umożliwiający swobodne korzystania z nich osobom niepowołanym. Takie okoliczności w rozpoznawanej sprawie nie zostały przez pozwanego wykazane. Ponownie należy podkreślić, że powódka padła ofiarą przestępstwa, na tyle dobrze przygotowanego, że nie ustrzegło się przed nim wiele innych osób.

Błędny jest przy tym pogląd, iż istotne znaczenie ma fakt dwukrotnego podania kodów jednorazowych. Oczywiste jest, iż powódka – logując się ponownie w dniu 23 maja 2014 roku nie wiedziała o dokonaniu nieautoryzowanej wypłaty z jej konta oszczędnościowego i nadal nie podejrzewała, że nie łączy się drogą elektroniczną z Bankiem. Reakcja powódki w dniu 27 maja 2014 roku – niezwłoczne powiadomienie pozwanego i policji o stwierdzonych transakcjach dokonanych bez woli i wiedzy powódki, świadczy również o braku z jej strony rażącego niedbalstwa. W tych okolicznościach uznać należy, że Sąd Rejonowy prawidłowo ocenił, iż transakcje dokonane z konta powódki nie były autoryzowane, ponieważ nie jest autoryzowaną taka transakcja, której dokonano przy użyciu instrumentu płatniczego należącego do płatnika i dokonano uwierzytelnienia, ale proces ten został dokonany bez zgody płatnika. Słusznie także przyjął, że powódka naruszyła art. 42 ust. 2 ustawy o usługach płatniczych, co oznacza, że winna ponieść odpowiedzialność za nieautoryzowane przelewy z jej konta do wysokości odpowiadającej 150 euro,ale nie można jej przypisać rażącego niedbalstwa.

Podzielić należy również pogląd Sądu Rejonowego, iż sformułowana w odpowiedzi na pozew teza dowodowa, co do której miałby zostać przeprowadzony dowód z opinii biegłego dotyczyła bądź faktów, które nie mogą być przedmiotem takiego dowodu, bądź okoliczności, które nie miały znaczenia dla rozstrzygnięcia. Jak już wyżej wskazano, powołani przez stronę pozwaną świadkowie szczegółowo przedstawili, jak mógł przebiegać atak cyberprzestępców, którego ofiarą padła powódka i inni klienci banku. Świadkowie ci wskazali również – przede wszystkim M. K., iż wyglądu strony internetowej, która wyświetliła się powódce w dniach 22 i 23 maja 2014 roku, nie da się obecnie dokładnie odtworzyć, ale że najczęściej nie odbiegała od wyglądu właściwej strony internetowej banku. Zeznania świadków, którzy zajmowali się analizą podobnych przypadków, a przede wszystkim zdarzenia, które było przedmiotem tej sprawy, słusznie zostały przez Sąd ocenione jako wystarczające do dokonania ustaleń faktycznych niezbędnych do rozstrzygnięcia.

Wobec powyższych okoliczności Sąd Okręgowy na podstawie art.385 k.p.c. oddalił apelację pozwanego.

O kosztach postępowania Sąd Okręgowy orzekł na podstawie art.98 k.p.c. uwzględniając wynik postępowania.Na koszty procesu zasądzone na rzecz powódki w tym przypadku złożyły się koszty zastępstwa procesowego powódki określone zgodnie punktem 5§6,§ 13 ust.1 pkt1 rozporządzenia Ministra Sprawiedliwości z dnia 28 września 2002

roku w sprawie opłat za czynności adwokackie oraz ponoszenia przez Skarb Państwa kosztów nieopłaconej pomocy prawnej udzielonej z urzędu (t.jedn. Dz.U. z 2013 poz.461 ze zm.).