Sygn. akt II Ca 426/17

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 24 sierpnia 2017 r.

Sąd Okręgowy w Białymstoku II Wydział Cywilny Odwoławczy

w składzie:

Przewodniczący:	SSO Renata Tabor (spr.)
Sędziowie:	SSO Elżbieta Siergiej SSO Mirosław Trzaska
Protokolant:	stażysta Sylwia Zbróg

po rozpoznaniu w dniu 10 sierpnia 2017 r. w Białymstoku

na rozprawie

sprawy z powództwa S. L. i D. L.

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

o zapłatę

na skutek apelacji powodów

od wyroku Sądu Rejonowego w Białymstoku

z dnia 3 marca 2017 r. sygn. akt XI C 2326/15

I. ***oddala apelację;***

II. ***zasądza od powodów solidarnie na rzecz pozwanego kwotę 2.700 (dwa tysiące siedemset) złotych tytułem zwrotu kosztów postępowania odwoławczego.***

UZASADNIENIE

Powodowie S. L. i D. L. wnieśli o zasądzenie od pozwanej (...) Bank (...) S.A. z siedzibą w W. na ich rzecz kwoty 14.801,73 euro wraz z ustawowymi odsetkami od dnia 12.05.2015 r. do dnia zapłaty. Nadto wnieśli o zasądzenie od pozwanego na ich rzecz kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych.

Pozwany (...) Bank (...) S.A. z siedzibą w W. wniósł o oddalenie powództwa w całości oraz zasądzenie solidarnie od powodów na rzecz pozwanego zwrotu kosztów postępowania, w tym kosztów zastępstwa procesowego według norm przepisanych.

Wyrokiem z dnia 31 marca 2017 roku Sąd Rejonowy w Białymstoku w sprawie XI C 2326/15 oddalił powództwo /pkt I/; zasądził od powodów solidarnie na rzecz pozwanego kwotę 3.934 zł tytułem zwrotu kosztów procesu /pkt II/ oraz nakazał pobrać od powodów solidarnie na rzecz Skarbu Państwa – Sądu Rejonowego w Białymstoku kwotę 39,40 zł tytułem zwrotu poniesionych w sprawie wydatków /pkt III/.

Sąd I instancji ustalił, że powodowie S. L. i D. L. w dniu 16.07.2012 r. zawarli z pozwanym (...) Bank (...) S.A. umowę o prowadzenie rachunków oszczędnościowych płatnych na żądanie, w oparciu o którą prowadzony jest rachunek nr (...). Dodatkowo strony w dniu 04.03.2014 r. zawarły umowę rachunku oszczędnościowo-rozliczeniowego Konto P. (...) usług bankowości elektronicznej oraz karty debetowej, w oparciu o którą prowadzony jest rachunek nr (...).

W dniu 11.05.2015 r. o godz. 10:54 powód próbował zalogować się na swoje konto poprzez stronę internetową (...). W tym czasie, podczas logowania powoda, został zdefiniowany nowy szablon odbiorcy o następujących danych: numer rachunku z: (...), numer rachunku na: (...), nazwa odbiorcy: D. K., tytułu płatności: (...). Dyspozycja powyższa została autoryzowana kodem nr (...) z karty kodów jednorazowych o numerze (...), które pozostawały w wyłącznym posiadaniu powoda. Z uwagi na to, że podczas logowania przekierowano powoda na inną stronę, telefonicznie zgłosił on nieprawidłowości w logowaniu na stronę usług bankowości elektronicznej pozwanego banku. W dacie zdarzenia pozwany bank zmieniał szatę graficzną strony internetowej, można było równolegle korzystać ze starej i nowej. Powód korzystał ze starej wersji. Podczas rozmowy telefonicznej powód nie wskazywał na inne problemy bądź nietypowe żądania ze strony banku lub innych wyświetlanych na jego komputerze. Po potwierdzeniu przez pracownika prawidłowości logowania i tego, że serwis działa prawidłowo, a konto powodów nie zostało zablokowane – powód zakończył rozmowę i kontynuował proces logowania do bankowości internetowej. Następnie powód po raz drugi o godz. 11:07 wykonał telefon do pozwanego ponownie zgłaszając pracownikowi pozwanego problemy w logowaniu do bankowości internetowej. Powód potwierdził podczas rozmowy, iż w trakcie prób logowania na stronie internetowej banku wyświetlił się symbol kłódki zabezpieczającej. Powód uzyskał od pracownika pozwanego potwierdzenie, że jego logowanie jest zatem bezpieczne. O godz. 13:44 powód poinformował pracownika banku, iż z jego konta dokonano nieautoryzowanych przelewów i zlecił zablokowanie wszystkich jego kont w pozwanym banku, co też pracownik pozwanego uczynił.

Powodowie niezwłocznie w dniu 11.05.2015 r. zgłosili szkodę z tytułu nieautoryzowanych przelewów i wnieśli o anulowanie wszystkich transakcji z dnia 11.05.2015 roku. Nadto powód dokonał anulowania transakcji nieautoryzowanych, zablokowanie kont, wymiany loginów i zmiany haseł dostępu do środków finansowych zgromadzonych na instrumentach pozwanego w ramach umowy z powodami. Powód zgłosił dodatkowo informację na Policję, gdzie do chwili obecnej jest prowadzone postępowanie KW (...).

W dniu 11.05.2015 r. w godz. 12:46 do 13:39 dokonano z konta powodów czterech transakcji nieautoryzowanych w kwocie: I transakcja – 4.932,23 euro, II transakcja – 4.914,56 euro, III transakcja – 4.954,94 euro, IV transakcja – 5.002,90 euro. Pieniądze w walucie euro przelewane były z rachunku bieżącego powodów na rachunek oszczędnościowo- rozliczeniowy prowadzony w walucie PLN z automatycznym przewalutowaniem poprzez zdefiniowany wcześniej nowy szablon, z którego następnie zostały przelewane na rachunek przestępcy. Pozwany dokonał zwrotu tylko ostatniej z czterech nieautoryzowanych operacji – w kwocie 5.002,90 euro przewalutowanej na kwotę 19.800 zł na konto powodów.

Sąd I instancji zaznaczył, że powyższy stan faktyczny ustalił w oparciu o zgromadzone w sprawie dokumenty i nagrania rozmów zarejestrowanych na płytach CD, które nie były w sprawie kwestionowane przez żadną ze stron, zaś ich prawdziwość i wiarygodność nie budziła wątpliwości, a także w oparciu o zeznania świadków E. N., A. D. i J. G., uznanym za wiarygodne. Zeznania świadków A. D. i E. N. potwierdziły jedynie twierdzenia przedstawione przez powoda, były zbieżne z zapisami rozmów z płyt CD znajdującymi się w aktach sprawy. Natomiast świadek J. G. przedstawiła jedynie ogólny zarys mechanizmów działania osób dokonujących bezprawnych działań, których celem jest uzyskanie dostępu do rachunku bankowego innej osoby oraz procedury obowiązujące w pozwanym banku w zakresie zgłaszanych problemów czy ataków z uwagi na to, że szczegółowe ujawnienie tej procedury mogłoby zagrozić

bezpieczeństwu banku. Za miarodajny w sprawie Sąd I instancji uznał też dowód z opinii biegłego sądowego z zakresu M. K., choć opinia ta nie rozstrzygnęła okoliczności, w jakich doszło do pozyskania przez osobę trzecią haseł dostępu do kodów. Biegły mógł bowiem swoje ustalenia poczynić w sposób stanowczy jedynie w ograniczonym zakresie. Brak możliwości zbadania dysku z komputera powodów uniemożliwiło ustalenie, czy komputer ten posiadał właściwe zabezpieczenia antywirusowe.

W swej opinii biegły wskazał, że bezpośrednią przyczyną utraty środków z konta powodów było podanie przez powoda (co najmniej) w sposób nieświadomy kodów jednorazowych, które umożliwiły późniejsze wyprowadzenie środków z konta powodów. Brak dysku komputera uniemożliwił biegłemu wskazanie, w jakich okolicznościach mogło to nastąpić, przy logowaniu się na których stronach. Biegły jednoznacznie wskazał też, że nie doszło do złamania przez hakera zabezpieczeń na stronie banku, co wskazuje z kolei, że (jeśli wykluczyć celowe przekazanie kodów przez powoda osobie trzeciej i ich kradzież) podanie tych kodów nastąpiło podczas logowania się przez powoda na „podstawioną" przez hakera stronę udającą stronę banku.

W świetle powyższych okoliczności Sąd Rejonowy stwierdził, że decydujące dla wyniku procesu było ustalenie przede wszystkim działań powoda i ich ocena z punktu widzenia dochowania należytej staranności, a także ewentualnego zawinienia pozwanego w opisywanym zdarzeniu. Równocześnie Sąd ten stwierdził też, że bezpośrednią przyczyną utraty środków pieniężnych na rachunku powodów był fakt, że nieuprawniona osoba trzecia dokonała zdefiniowania nowego szablonu odbiorcy na przestępczy rachunek odbiorcy, który następnie został wykorzystany do realizacji na jego podstawie zakwestionowanych przez powodów przelewów. Nieustalona do tej pory osoba trzecia dokonała wyprowadzenia pieniędzy z konta powodów.

W ocenie Sądu I instancji – wbrew twierdzeniom strony powodowej – informacje przekazywane przez powoda podczas dwóch rozmów telefonicznych z przedstawicielem banku w godz. 10:51 i 11:07 nie pozwoliły pracownikowi podjąć wiedzy, że istnieje możliwość ataku hakerskiego na konto powodów oraz że podstawiono powodowi fałszywą stronę bankową do dokonywania przelewów. Powód nie przekazał wówczas informacji, którą posiadał i nie wskazał, że przy próbie logowania na swoje konto bankowe podał kod jednorazowy, bądź że podał ten kod po raz drugi dokonując jednego przelewu, co mogło pozwolić na wykorzystanie tego kodu przez inne osoby, do czego rzeczywiście później doszło. Poza ustaleniem, że na pewno do przekazania kodu doszło, nie istnieje możliwość jednoznacznego określenia metody pozyskania przez osobę trzecią haseł dostępu do kodów z uwagi na brak jednoznacznego stanowiska powoda w tej kwestii, a także tego, że na podstawie zgromadzonego w sprawie materiału dowodowego nie jest to możliwe.

Powód nie kwestionował, że podczas rozmów z pracownikami banku nie mówił o udostępnieniu kodów bądź użyciu ich w sytuacji nietypowej. Wynika to jednoznacznie z dołączonych nagrań, a także z zeznań świadek E. N.. Na skutek tego pracownik banku podjął wszelkie działania mające na celu sprawdzenie zasadności zgłoszonego żądania. Wówczas zostało sprawdzone hasło i konto – czy nie zostały zablokowane. Sama informacja, że strona automatycznie przelogowuje się na stronę nową nie była nietypowa bądź budząca wątpliwości, gdyż wówczas w pozwanym banku obowiązywały równolegle dwa systemy. Żadnych innych wątpliwości, problemów, czy nietypowych żądań powód nie zgłaszał. Z zeznań świadek J. G. – eksperta w zespole monitoringu i autoryzacji operacji Banku (...) S.A. – wynika, że w pozwanym banku obowiązują specjalne procedury w przypadku wystąpienia podejrzenia zamachu na bezpieczeństwo kont klientów. Mając na uwadze, że pracownik banku (...) podczas rozmowy telefonicznej z powodem uzyskała cząstkowe informacje o problemie i swoje działania mogła oprzeć tylko na nich, podjęła stosowne procedury w niniejszej sytuacji, sprawdziła stan konta powoda, który nie nasuwał żadnych wątpliwości. Gdy powód podczas trzeciej rozmowy z przedstawicielem pozwanego wskazał, że „uciekają mu z konta pieniądze" pracownicy banku zareagowali natychmiast, świadek A. D. nie czekając nawet na reakcję infolinii założyła blokadę na konto powodów. Świadek J. G. zeznała, że na podstawie elektronicznego zapisu wszystkich czynności na rachunku klienta (tu: powoda), tzw. togach systemowych wynika, że po zalogowaniu na stronę internetową utworzony został szablon płatności potwierdzony kodem z karty kodów będącej w posiadaniu powoda. Nie byłoby możliwości dokonania tej transakcji (dzięki której następnie doszło do nieuprawnionego wyprowadzenia pieniędzy z konta) bez potwierdzenia przez kod z karty kodów. Tak więc powód był zobowiązany do podania kodu z karty kodów w sytuacji niezwiązanej z dokonywaniem transakcji, który posłużył do stworzenia szablonu umożliwiającego dokonywanie przelewów bez

potrzeby każdorazowej autoryzacji kodem i podał go pomimo tego, że nie powinien. Podał nie zachowując należytej ostrożności, którą w tej sytuacji szczególnie winien wzbudzić mając na uwadze bariery, które napotykał podczas logowania. Przedstawiony przez świadka mechanizm koreluje z wnioskami zawartymi w opinii biegłego sądowego z zakresu informatyki M. K.. Biegły wprawdzie wskazał, że nie podstawie przedstawionego materiału dowodowego nie istnieje możliwość jednoznacznego określenia metody pozyskania przez osobę trzecią haseł dostępu do kodów autoryzacyjnych, ale brak jednoznaczności zachodzi jedynie jeśli chodzi o moment wpisania przez powoda kodu, którym posłużył się haker, chociaż biegły zaznaczył, że prawdopodobnie nastąpiło to w trakcie logowania do systemu bankowego w celu dokonanie jednego z 8 przelewów wychodzących w dniu 11.05.2015 r. przed godziną 10:54. Fakt, że powód będąc zalogowany na swoim koncie wpisał kod, nie budzi żądnych wątpliwości. Biegły wskazał też, że nie może być mowy o wadliwym zabezpieczeniu po stronie banku, bowiem nie nastąpiło przełamanie zabezpieczeń systemu bankowego, został podany poprawny login i hasło w celu zalogowania się na konto, a do założenia nowego szablonu odbiorcy został użyty prawidłowy kod jednorazowy nr (...).

W ocenie Sądu I instancji, powód, który wcześniej wielokrotnie logował się na swoje konto, miał wiedzę że nie powinien podawać kodów jednorazowych podczas logowania i że podaje się tylko jeden kod podczas danej transakcji oraz że nie wyświetlają się komunikaty o podanie dodatkowego kodu podczas innych czynności, niż autoryzowanie przelewu. Takie zalecenia cały czas widnieją na stronie internetowej logowania, a poza tym powodowi nigdy wcześniej powodowi nie wyświetlały się na etapie logowania bądź dokonywania operacji na koncie podobne żądania. Powód pomimo wiedzy odnośnie do braku takiego obowiązku wpisał jeden z posiadanych kodów podczas logowania bądź będąc na koncie bez dokonywania stosownych ku temu transakcji, a potem nie powiedział o tym pracownikowi banku, przeciwnie – skupił swoje rozmowy na tym, że otwiera mu się automatycznie nowa strona do logowania. Pozwany poinformował powoda, że od jakiegoś czasu funkcjonują dwie strony banku, tj. stara używana do tej pory i nowa. Jednakże nie wzbudził zwiększonej czujności powoda fakt, że występowanie dwóch stron od pewnego czasu nie powodowało wcześniej jego automatycznego przekierowania na inną stronę, a tym samym powód przed logowaniem się na stronę nie zweryfikował w sposób dokładny od strony wizualnej i merytorycznej strony logowania, zwłaszcza że – jak sam przyznał podczas rozmowy – wcześniej dostał maila z zawirusowanym załącznikiem, którzy otworzył, miał potencjalną świadomość, że jego komputer może być zawirusowany, a to może prowadzić do ataków hakerskich. Pierwsza wzmianka o tym, że powód ma wirus w komputerze nastąpiła dopiero podczas połączenia ok. godz. 13:00 i poinformowaniu, że znikają powodowi pieniądze z konta. Powodowie nie udowodnili, że na komputerze, z którego były dokonywane przedmiotowe przelewy było zainstalowane oprogramowanie antywirusowe (na pewno nie jest wystarczającym dowodem ku temu przedłożony przez powodów certyfikat dotyczący zakupu programu antywirusowego, bowiem sam fakt zakupu programu nie jest równoznaczny z zainstalowaniem go i używaniem na komputerze), powodowie nie przedstawili dysku do zbadania pomimo żądania ze strony sądu na wniosek strony pozwanej. Pomimo wcześniejszego deklarowania, że dysk ten znajduje się w ich posiadaniu, w późniejszym czasie powodowie wskazali, że został on utracony. W związku z tym brak było możliwości zbadania tego dysku przez biegłego i ustalenia, czy powodowie posiadali zainstalowany i zaktualizowany program antywirusowy oraz okoliczności związanych z ewentualnym zawirusowaniem ich komputera.

Przywołując treść art. 42 oraz 46 ust. 1 i 3 ustawy o usługach płatniczych, a także § 12 ust. 3 i § 13 regulaminu świadczenia usług bankowości elektronicznej w (...) Banku (...) S.A., Sąd Rejonowy stwierdził, że zachowanie powoda podczas logowania w dniu 11 maja 2015 r. było obarczone podwójnym rażącym niedbalstwem z jego strony. Przede wszystkim polegało ono na tym, że powód podczas logowania bądź używania serwisu spotkał się z nietypowym w takiej sytuacji komunikatem, by podał jednorazowy kod do autoryzacji. Powód pomimo tego, że nie powinien był, wpisał ten kod. Następnie zaś nie poinformował konsultanta podczas rozmowy, ani w inny sposób nie zawiadomił pozwanego, że został poproszony o podanie dodatkowego kodu autoryzacyjnego i go wpisał, dzięki czemu naprowadziłby pozwanego na konieczność podjęcia stosownych środków ostrożności. Powód swoje dwukrotne zgłoszenia oparł przede wszystkim na zgłaszaniu pracownikowi pozwanego banku informacji o automatycznym przekierowaniu na nową stronę banku. Powód nie zgłosił swoich wątpliwości co do autentyczności strony pozwanego – (...), które mogły mu się nasunąć z uwagi na świadomość, że jego komputer może być zawirusowany, zwłaszcza że pracownik banku podczas pierwszej rozmowy pytał powoda, czy sam wpisywał adres strony czy stronę otworzył z „maila", tj. na skutek wejścia w link z

adresem strony przesłany drogą mailową. Poza tym powód nie przedstawił dowodów, że sprzęt, na którym dokonywał on przelewów, był w odpowiedni sposób zabezpieczony antywirusowo. Tym samym powód w ocenie Sądu I instancji naruszył w/w art. 42 ust. 1 ustawy, bowiem nie zgłosił niezwłocznie dostawcy nieuprawnionego użycia instrumentu płatniczego w postaci kodu autoryzacyjnego, przez co pracownik banku nie powziął wątpliwości co do możliwości wystąpienia ataku hakerskiego na konto powodów i nie podjął natychmiastowych kroków w celu jego zablokowania.

W konsekwencji Sąd Rejonowy uznał, że to powód wskutek rażącego niedbalstwa naruszył obowiązek korzystania z instrumentu płatniczego zgodnie z umową, a także obowiązek niezwłocznego zgłaszania nieuprawnionego użycia instrumentu płatniczego, tj. kodu jednorazowego. Nie można natomiast mówić o jakimkolwiek zaniedbaniu ze strony pozwanego, zwłaszcza obowiązków wynikających z art. 43 ust. 1 ustawy. Bank nie umożliwił bowiem innym niż użytkownik uprawniony korzystania z indywidualnych zabezpieczeń instrumentu płatniczego powoda, przyjmował zgłoszenia powoda i reagował odpowiednio do ich treści. Powództwo podlegało zatem oddaleniu.

O kosztach procesu Sąd I instancji orzekł na podstawie art. 98 § 1 i 3 kpc, zgodnie z zasadą odpowiedzialności za rezultat procesu.

Apelację od powyższego wyroku złożyli powodowie S. L. i D. L. zaskarżając go w całości oraz zarzucając mu:

I. ***naruszenie prawa materialnego, a mianowicie:***

1) ***art. 471 kc, poprzez jego niezastosowanie, skutkujące pominięciem niewłaściwego wykonania umowy przez pozwany bank, polegającego na tym, że bank pomimo zgłoszenia przez powoda w dniu 11 maja 2015 roku o godz. 11.54 uzasadnionych wątpliwości co do funkcjonowania strony bankowości internetowej pozwanego, nie podjął żadnych działań zmierzających do wprowadzenia procedur zapobiegających atakowi hakerskiemu, a pracownik banku – nieprzeszkolony w zakresie bezpieczeństwa – zapewnił powoda o bezpiecznym użytkowaniu i nie przekierował go do komórki bezpieczeństwa pozwanego, co doprowadziło do przeprowadzenia ataku hakerskiego tego dnia o godz. 13.00;***

2) ***art. 725 kc, poprzez jego niezastosowanie skutkujące pominięciem, że przez umowę rachunku bankowego bank będąc zobowiązany względem powodów do przechowywania ich środków pieniężnych nie dochował ciążącego na nim obowiązku zapewnienia bezpieczeństwa depozytów, co skutkowało wypłatą środków zgromadzonych na rachunku powodów do rąk osób nieuprawnionych;***

3) ***art. 6 kc, poprzez błędne przyjęcie, że pozwany wykazał zgodnie z ciążącym na nim obowiązkiem, iż podjął jakiekolwiek działania w odpowiedzi na zgłoszenia powoda w dniu 11 maja 2015 roku o godz. 10.54 i 11.07, podczas gdy pracownik banku – nieprzeszkolony w zakresie bezpieczeństwa – zapewnił powoda o bezpiecznym użytkowaniu i nie przekierował go do komórki bezpieczeństwa pozwanego, a działania, które bank podjął po godz. 13.00 w wyniku zawiadomienia przez powoda już po utracie środków zgromadzonych na rachunku, były spóźnione, zatem pozwany wykazał, że nie podjął żadnych działań z uwagi na brak procedur obowiązujących u pozwanego, co skutkowało błędnym przyjęciem, że to powód odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości;***

4) ***art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (t.j. Dz.U. 2016, poz. 1572 z późn. zm.), poprzez błędne przyjęcie, że logowanie powoda w dniu 11 maja 2015 roku było obarczone podwójnym niedbalstwem z jego strony w sytuacji, gdy Sąd stwierdził, że poza ustaleniem, iż doszło do przekazania kodu, nie istnieje możliwość określenia metody jego pozyskania, a na podstawie zgromadzonego w sprawie materiału dowodowego nie jest to możliwe,***

co skutkowało błędnym przyjęciem, że to powód odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości;

5) ***art. 42 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (t.j. Dz.U. 2016, poz. 1572 z późn. zm.), poprzez błędną wykładnię skutkującą przyjęciem, że powód nie wykazał, iż zgłosił dostawcy podejrzenie nieuprawnionego użycia instrumentu, a pracownik pozwanego nie powziął wątpliwości co do atak hakerskiego w sytuacji, gdy powód w dniu 11 maja 2015 roku już o godz. 10.54 i o godz. 11.07 zgłaszał pozwanemu bankowi jako profesjonaliście problemy z dostępem do usług bankowości elektronicznej, wskutek czego powód nie dopuścił się naruszenia obowiązków wynikających z w/w regulacji, lecz to brak reakcji ze strony banku na zgłoszenia powoda doprowadził do nieautoryzowanych transakcji i utraty środków z konta powodów tego samego dnia;***

6) ***art. 45 ust. 1 i 2 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (t.j. Dz.U. 2016, poz. 1572 z późn. zm.), poprzez błędną wykładnię pojęcia rażącego niedbalstwa powoda w naruszeniu obowiązków wynikających z art. 42 wspomnianej ustawy;***

7) ***art. 43 ust. 1 ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych (t.j. Dz.U. 2016, poz. 1572 z późn. zm.), poprzez błędne przyjęcie, że po stronie pozwanego nie nastąpiło zaniedbanie w wykonaniu ciążącego na nim obowiązku w sytuacji, gdy powód w dniu 11 maja 2015 roku o godz. 10.54 i o godz. 11.07 zgłosił problemy w dostępie do usług bankowości elektronicznej, a pozwany jako profesjonalista nie umożliwił korzystania z instrumentu płatniczego po dokonaniu zgłoszenia zgodnie z art. 42 ust. 1 pkt 2 w/w ustawy w sposób zapewniający bezpieczeństwo środków powodów;***

II. ***naruszenie przepisów postępowania, a mianowicie:***

1) ***art. 233 kpc, poprzez dowolne uznanie, że w niniejszej sprawie brak było dowodu, iż bank postąpił niezgodnie z procedurami służącymi ochronie środków zgromadzonych na koncie powodów w sytuacji, gdy z opinii biegłego sądowego wynika, że „pozwany w którymś momencie uznał wątpliwości powoda za uzasadnione i podjął czynności w celu ochrony interesów klienta zgodnie z obowiązującymi u pozwanego procedurami", wskutek czego błędnie przyjęto brak odpowiedzialności banku wobec zgłaszania przez powoda w dniu 11 maja 2015 roku o godz. 10.54 i 11.07 problemów z dostępem do usług bankowości elektronicznej, a więc jeszcze kilka godzin przed utratą środków z konta powodów;***

2) ***art. 233 § 1 kpc, poprzez dowolną ocenę dowodów skutkującą pominięciem, że pozwany nie przestrzegał obowiązujących u niego procedur w przypadku podejrzenia ataku hakerskiego mimo zeznań pracownika pozwanego, że po zawiadomieniach przez powoda o godz. 10.54 i 11.07 nie podjął żadnych czynności mających na celu zabezpieczenie środków powodów, co skutkowało błędnym przyjęciem braku odpowiedzialności pozwanego banku;***

3) ***art. 233 § 1 kpc, poprzez wyprowadzenie z materiału dowodowego wniosków z niego niewypływających, w tym wniosku, że zeznania świadków nie dają podstaw do przyjęcia odpowiedzialności pozwanego banku w zakresie roszczeń powodów, choć świadek A. D. zeznała, że „po informacji powoda weszła na konto i zobaczyła, że żadne blokady nie są założone, więc je założyła", co jednoznacznie potwierdzało, iż bank miał możliwość reakcji i mógł zapobiec nieautoryzowanym transakcjom, a po zgłoszeniach powoda jego wątpliwości co do działania systemu pozwany jako profesjonalista nie podjął żadnych działań;***

4) ***art. 233 kpc, poprzez przyjęcie niezgodnie z zasadami doświadczenia życiowego i logiki, że do ujawnienia kodu jednorazowego dostępu mogło dojść w wyniku zachowania powoda, podczas gdy***

brak jest dowodów na okoliczność stosowanych środków, technologii i procedur oraz sposobów zabezpieczenia stron internetowych banku, trybu i sposobu otrzymania przez klienta poufnego identyfikatora oraz trybu udostępniania haseł do kanałów dostępu przez bank;

5) ***art. 233 § 1 kpc w zw. z art. 328 § 2 kpc, poprzez brak wszechstronnego rozważenia materiału dowodowego i niewskazanie w uzasadnieniu wyroku, jakich wymogów dotyczących ochrony instrumentu płatniczego powód nie dochował, a ograniczenie się tylko do domniemania, że powód nie zgłosił nieuprawnionego użycia kodu jednorazowego;***

6) ***art. 233 kpc, poprzez dowolne przyjęcie, że informacje przekazane przez powoda w dwóch rozmowach telefonicznych z pozwanym (o godz. 10.54 i 11.07) nie pozwoliły na zablokowanie konta powodów przez pracownika banku w sytuacji, gdy biegły sądowy wskazał, iż „w momencie, gdy rozmowa dotyczy problemów z logowaniem się oraz problemów z przełączaniem ze starego serwisu na nowy, wzmianka powoda o karcie kodów w kontekście logowania powinna wzbudzić czujność pracownika banku i odpowiednią reakcję", co skutkowało błędnym przyjęciem braku odpowiedzialności banku;***

7) ***art. 233 kpc, poprzez dowolne przyjęcie, że powodowie nie udowodnili istnienia na ich komputerze programu antywirusowego w sytuacji, gdy z opinii biegłego sądowego wynika, iż „powód miał wykupioną licencję na oprogramowanie antywirusowe, nie istnieje przyczyna, dla której oprogramowanie do miałoby nie miałoby być zainstalowane na komputerze powoda" oraz, że „z dostępnego materiału dowodowego nie wynika jednoznacznie, żeby komputer powoda był zainfekowany wirusem";***

8) ***art. 326 § 1 kpc, poprzez ogłoszenie wyroku po upływie dwóch tygodni od zamknięcia rozprawy;***

III. ***sprzeczność istotnych ustaleń Sądu z treścią zebranego w sprawie materiału dowodowego wskutek naruszenia przepisów postępowania, które miało wpływ na wynik sprawy, a mianowicie art. 233 § 1 kpc, poprzez:***

1) ***przyjęcie, że dowód z opinii biegłego informatyka nie rozstrzygnął, w jakich okolicznościach doszło do pozyskania przez osobę trzecią haseł dostępu i kodu przy jednoczesnym oparciu rozstrzygnięcia o tę opinię;***

2) ***przyjęcie, że biegły sądowy z zakresu informatyki wskazał, iż bezpośrednią przyczyną utraty środków z konta powodów było podanie przez powoda w sposób nieświadomy kodów jednorazowych, które umożliwiły późniejsze wyprowadzenie środków z konta powodów w sytuacji, gdy z opinii biegłego wynika wprost, że ze względu na brak dysku powoda nie ma możliwości potwierdzenia lub zaprzeczenia tej wersji oraz że nie wynika jednoznacznie, by dysk powoda był zainfekowany, co skutkowało błędnym przyjęciem odpowiedzialności powodów;***

3) ***przyjęcie, że biegły jednoznacznie wskazał, iż na gruncie niniejszej sprawy nie może być mowy o wadliwym zabezpieczeniu po stronie banku, bowiem nie nastąpiło przełamanie zabezpieczeń systemu bankowego, podczas gdy w zebranym materiale dowodowym brak jest dowodów na okoliczność środków, technologii i procedur oraz sposobu zabezpieczenia stron internetowych pozwanego.***

Mając na uwadze powyższe, powodowie wnosili o zmianę zaskarżonego wyroku poprzez uwzględnienie powództwa w całości oraz zasądzenie od pozwanego na ich rzecz kosztów procesu za obie instancje wg norm przepisanych, ewentualnie o uchylenie zaskarżonego wyroku i przekazanie sprawy Sądowi I instancji do ponownego rozpoznania z pozostawieniem temu Sądowi rozstrzygnięcia o kosztach procesu za obie instancje.

Sąd Okręgowy zważył, co następuje:

Apelacja powodów nie zasługiwała na uwzględnienie.

W ocenie Sądu Okręgowego ustalenia faktyczne, poczynione przez Sąd I instancji, są prawidłowe. Sąd Okręgowy w pełni je podziela i przyjmuje za własne. Sąd Rejonowy dokonał wszechstronnej, prawidłowej analizy materiału dowodowego i na tej podstawie wysnuł trafne wnioski. Podniesione w apelacji powodów zarzuty, kwestionujące zasadność rozstrzygnięcia i wskazujące na naruszenie przepisów prawa procesowego i materialnego, nie mogły tym samym skutkować zmianą zaskarżonego orzeczenia w postulowany przez skarżących sposób.

W pierwszej kolejności należy zdaniem Sądu Okręgowego zauważyć, że apelacja powodów w znacznej mierze sprowadzała się do zarzutów dotyczących analizy zgromadzonego w sprawie materiału dowodowego, tj. do zarzutu naruszenia art. 233 § 1 kpc m.in. poprzez „dowolne uznanie, że w niniejszej sprawie brak było dowodu, iż bank postąpił niezgodnie z procedurami służącymi ochronie środków zgromadzonych na koncie powodów w sytuacji", mimo że dowodem takim była opinia biegłego sądowego, a także poprzez pominięcie, że pozwany bank nie wykazał przestrzegania procedur przewidzianych w przypadku podejrzenia ataku hakerskiego, choć niewdrożenie takich procedur wynikało zarówno z rozmów powoda z pracownikami banku przeprowadzanych w dniu 11 maja 2015 roku, jak i z dowodu z zeznań świadków. Skarżący zarzucali też w apelacji błędną ocenę materiału dowodowego odnośnie do niezachowania przez nich wymogów ochrony instrumentu płatniczego, jak również pominięcie szeregu wniosków poczynionych przez biegłego sądowego z zakresu informatyki M. K.. Skutkować to zaś miało błędnym uznaniem, że pozwany bank nie ponosi odpowiedzialności za nieautoryzowane transakcje, w wyniku których powodowie utracili z ich rachunku bankowego dochodzoną pozwem kwotę. Odnosząc się zatem do tych zarzutów trzeba zdaniem Sądu Okręgowego zaznaczyć, że wbrew odmiennym twierdzeniom apelacji Sąd I instancji prawidłowo i bardzo wnikliwie ocenił zebrany w sprawie materiał dowodowy. Nie przekroczył przy tym granic określonych w art. 233 § 1 kpc, a także właściwie ustalił wszystkie istotne dla sprawy fakty. Należy zauważyć, że skuteczne postawienie zarzutu naruszenia przez Sąd wspomnianego art. 233 § 1 kpc wymaga wykazania, że Sąd ten uchybił zasadom logicznego rozumowania lub doświadczenia życiowego. To bowiem jedynie może być przeciwstawione uprawnieniu sądu do dokonywania swobodnej oceny dowodów. Natomiast nie jest wystarczające przekonanie strony o innej niż przyjął sąd wadze (doniosłości) poszczególnych dowodów i ich odmiennej ocenie niż ocena sądu (tak Sąd Najwyższy w wyroku z dnia 6 listopada 1998 roku, sygn. akt: II CKN 4/98, niepubl.). Skarżący zaś, zarzucając Sądowi I instancji uchybienie artykułowi 233 § 1 kpc, nie wykazali jednak naruszenia wspomnianych wyżej zasad logicznego rozumowania lub doświadczenia życiowego przy ocenie poszczególnych dowodów, a ich zarzuty stanowiły jedynie polemikę z ustaleniami i wnioskami tego Sądu. Innymi słowy, w ocenie Sądu Okręgowego powodowie starali się zatem jedynie podważyć w ten sposób dokonaną przez Sąd Rejonowy analizę materiału dowodowego odnośnie do wymienionych wyżej kwestii, jednakże przeciwstawiając dokonaną ocenę dowodów z tym, co według ich subiektywnego odczucia Sąd I instancji winien był orzec, nie zdołali oni wykazać jakiejkolwiek uchybienia ze strony tego Sądu. W konsekwencji należy zdaniem Sądu Okręgowego stwierdzić, że przeprowadzone w niniejszej sprawie postępowanie dowodowe nie odznaczało się żadnymi brakami. Poczynione przez Sąd Rejonowy wnioski były zaś właściwie i bardzo dokładnie, wręcz drobiazgowo, wyjaśnione, co dotyczy także oceny dowodów z zeznań wspomnianych wyżej świadków – pracowników pozwanego – jako że zeznania te nie zostały skutecznie podważone przez skarżących. Tym samym nie było zdaniem Sądu Okręgowego podstaw, by dokonywać oceny dowodów przedstawionych w sprawie inaczej, niż uczynił to Sąd I instancji, podobnie jak nie było też podstaw, by uzasadnienie zaskarżonego wyroku uznawać za nieodpowiadające wymogom zawartym w art. 328 § 2 kpc.

Odnosząc się zaś ściśle do wzmiankowanej uprzednio kwestii oceny dowodu z opinii biegłego warto zdaniem Sądu Okręgowego zauważyć, że co do zasady sąd nie jest związany tą opinią i ocenia ją na podstawie wspomnianego wyżej art. 233 kpc. Swoistość tej oceny polega jednak na tym, że nie chodzi tu o kwestię wiarygodności, jak przy dowodzie z zeznań świadków i stron, lecz o pozytywne lub negatywne uznanie wartości rozumowania zawartego w opinii i uzasadnienie, dlaczego pogląd biegłego trafił lub nie do przekonania sądu. Z jednej strony, konieczna jest kontrola z punktu widzenia zasad logicznego rozumowania i źródeł poznania, z drugiej – istotną rolę odgrywa stopień zaufania do

wiedzy reprezentowanej przez biegłego. Sąd może oceniać opinię biegłego pod względem fachowości, rzetelności czy logiczności. Może pomijać oczywiste pomyłki czy błędy rachunkowe. Nie może jednak nie podzielać merytorycznych poglądów biegłego czy zamiast nich wprowadzać własne stwierdzenia (tak Sąd Najwyższy w orzeczeniu z dnia 19 grudnia 1990 roku, I PR 148/90, OSP 1991, nr 11–12, poz. 300).

Powyższe rozważania, czynione na gruncie regulacji przewidzianej w art. 233 kpc, pozostawały w ocenie Sądu Okręgowego kluczowe dla oceny zarzutów apelacji, jako że w rozpoznawanej sprawie sporny był nie tyle fakt ataku hakerskiego na rachunek bankowy powodów, ile kwestia naruszenia przez strony niniejszego procesu obowiązków, które taki atak miały uniemożliwiać. W tym kontekście należy zdaniem Sądu Okręgowego podkreślić, że choć strony łączyła umowa rachunku bankowego, znajdująca podstawę prawną m.in. w przywoływanym w apelacji art. 725 kc, to jednak wspomniana wyżej obowiązki stron oraz zasady odpowiedzialności banku za nieautoryzowane transakcje uregulowane zostały w ustawie z dnia 19 sierpnia 2011 roku o usługach płatniczych (t.j. Dz.U. 2016, poz. 1572 z późn. zm., dalej: ustawa). W związku z tym nie można pominąć, że zgodnie z art. 40 ustawy, transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą (ust. 1). Zgoda może dotyczyć także kolejnych transakcji płatniczych. Zgoda powinna być udzielona przez płatnika przed wykonaniem transakcji płatniczej albo kolejnych transakcji płatniczych, chyba że płatnik i jego dostawca uzgodnili, że zgoda może zostać udzielona także po ich wykonaniu (ust. 2). W myśl art. 41 ustawy, użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany korzystać z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu (ust. 1) przy czym w celu spełnienia obowiązku korzystania z instrumentu płatniczego zgodnie z umową ramową użytkownik, z chwilą otrzymania instrumentu płatniczego, podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych zabezpieczeń tego instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (ust. 2). Szereg obowiązków spoczywa także na dostawcy wydającym instrument płatniczy, który na mocy art. 43 ust. 1 ustawy obowiązany jest m.in. do zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, zapewnienia stałej dostępności odpowiednich środków pozwalających użytkownikowi na dokonanie zgłoszenia zgodnie z art. 42 ust. 1 […] czy zapewnienia procedur pozwalających na udowodnienie dokonania zgłoszenia, o którym mowa w art. 42 ust. 1, przy czym to dostawca ponosi ryzyko związane z wysłaniem płatnikowi instrumentu płatniczego lub jego indywidualnych zabezpieczeń. W dalszej kolejności należy zauważyć, że zgodnie z art. 44 ust. 1 ustawy, użytkownik niezwłocznie powiadamia dostawcę o stwierdzonych nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcjach płatniczych. W myśl art. 45 ustawy, ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika (ust. 1), przy czym 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 (ust. 2).

Co w rozpoznawanej sprawie istotne, art. 46 ustawy 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 (ust. 1). 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 posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub przywłaszczenia instrumentu płatniczego lub jego nieuprawnionego użycia w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2 (ust. 2). 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 (ust. 3). Po dokonaniu zgłoszenia zgodnie z art. 42 ust. 1 pkt 2 płatnik nie odpowiada za nieautoryzowane transakcje płatnicze, chyba że płatnik doprowadził umyślnie do nieautoryzowanej transakcji (ust. 4).

W świetle powyższych regulacji należy zatem zdaniem Sądu Okręgowego stwierdzić, że na powodach jako osobach korzystających z usług płatniczych w charakterze płatnika (art. 2 ust. 34 ustawy) i uprawnionych do korzystania z instrumentu płatniczego, rozumianego jako zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego (art. 2 ust. 10 ustawy), spoczywał szereg obowiązków, sprowadzających się w istocie do korzystania z instrumentu płatniczego zgodnie z umową ramową, zgłaszania nieuprawnionego dostępu do instrumentu płatniczego oraz podejmowania środków odnośnie do zabezpieczenia instrumentu płatniczego i nieudostępniania go osobom nieuprawnionym. W okolicznościach rozpoznawanej sprawy pierwszy z wymienionych wyżej obowiązków, tj. przestrzeganie umowy ramowej, sprowadzał się zaś w istocie do przyjętego w umowie obowiązku przestrzegania Regulaminu świadczenia usług bankowości elektronicznej w (...) S.A., co oznaczało z kolei obowiązek stosowania m.in. aktualnego oprogramowania antywirusowego i antyspamowego oraz zapory firewall, najnowszych wersji przeglądarek internetowych oraz haseł zabezpieczających przed nieuprawnionym dostępem do komputera osób trzecich. Zabezpieczanie instrumentu płatniczego obejmowało natomiast – wobec przytoczonej wyżej definicji zawartej w art. 2 ust. 10 ustawy – zarówno całą kartę kodów doręczoną powodom, jak i każdy poszczególny kod używany przy składaniu zlecenia płatniczego, czyli przy konkretnej pojedynczej transakcji. Nieprzestrzeganie powyższych obowiązków przez powodów jako płatników (w rozumieniu ustawy) w warunkach rażącego niedbalstwa skutkowało – w świetle jednoznacznej regulacji przewidzianej w art. 46 ust. 3 ustawy – tym, że to właśnie powodowie odpowiadaliby za nieautoryzowane transakcje płatnicze w pełnej wysokości, co jednocześnie zwalniałoby z odpowiedzialności za te transakcje pozwany bank. Zdaniem Sądu Okręgowego, biorąc pod uwagę powyższe sprecyzowanie okoliczności faktycznych kluczowych dla rozstrzygnięcia niniejszej sprawy w kontekście obowiązujących regulacji prawnych, należy jasno stwierdzić, że wspomniany przypadek rażącego niedbalstwa naruszenia przez powodów obowiązków wymienionych w art. 42 ustawy miał w istocie miejsce, co jednoznacznie wynika ze zgromadzonego w toku postępowania materiału dowodowego.

Przede wszystkim należy zdaniem Sądu Okręgowego zaznaczyć, że w rozpoznawanej sprawie nie budził wątpliwości fakt, iż w trakcie ewidentnego ataku hakerskiego mającego miejsce w dniu 11 maja 2015 roku systemy zabezpieczeń pozwanego banku nie zostały przełamane. Wynika to jednoznacznie z dopuszczonego przez Sąd I instancji dowodu z opinii biegłego sądowego z zakresu informatyki, który w tym właśnie zakresie w pełni zasługiwał na uznanie go za podstawę ustaleń faktycznych w sprawie. Jak już bowiem wspomniano, przy ocenie takiego właśnie dowodu nie chodzi bowiem o kwestię wiarygodności, lecz o pozytywne lub negatywne uznanie wartości rozumowania zawartego w opinii i uzasadnienie, dlaczego pogląd biegłego trafił lub nie do przekonania sądu. Biegły M. K. wyraźnie zaś wskazał, że swoje ustalenia mógł poczynić w sposób stanowczy jedynie w ograniczonym zakresie wobec braku możliwości zbadania dysku z komputera powodów, co oznacza innymi słowy, że biegły mógł się wypowiedzieć autorytatywnie tylko we wspomnianej wyżej kwestii przełamania systemów banku opierając się w tym zakresie na swej wiedzy fachowej. W konsekwencji w takim też tylko zakresie dowód z opinii biegłego mógł zostać uznany za miarodajny w sprawie, co zresztą stało się przedmiotem prawidłowej oceny przez Sąd I instancji. Biegły wskazał też jednak równocześnie, że skoro nie doszło do złamania przez hakera zabezpieczeń na stronie banku, to podanie kodów służących autoryzacji transakcji (zlecenia płatniczego), a tym samym udostępnienie instrumentu płatniczego osobom nieuprawnionym, nastąpiło podczas logowania przez powoda na „podstawioną" przez hakera stronę udającą stronę banku. Z wnioskiem tym, jako logicznym i pozostającym w zgodzie z zasadami doświadczenia życiowego, trudno w ocenie Sądu Okręgowego się nie zgodzić, zwłaszcza że znajduje on pełne potwierdzenie w zgromadzonym w sprawie materiale dowodowym.

Za równie niewątpliwy jak fakt nieprzełamania systemów bezpieczeństwa banku należy zdaniem Sądu Okręgowego uznać fakt, że powodowie nie wypełnili obowiązku przestrzegania umowy ramowej w zakresie stosowania aktualnego

oprogramowania antywirusowego. Fakt zawirusowania komputera powodów, na którym skarżący w dniu 11 maja 2015 roku próbował się logować do systemu pozwanego banku, został przez S. L. przyznany w rozmowie z pracownikiem pozwanego przeprowadzonej wyżej wspomnianego dnia ok. godziny 13.40, kiedy to powód zawiadamiał bank o znikaniu pieniędzy z konta. Skarżący sam zatem zorientował się już wówczas co do stanu rzeczy w tym zakresie, co w ocenie Sądu Okręgowego rodziło kwestię właściwego zabezpieczenia komputera poprzez stosowanie wspomnianego wyżej aktualnego oprogramowania antywirusowego. Sąd I instancji oceniając tę kwestię prawidłowo uznał, że o stosowaniu takiego oprogramowania nie mógł świadczyć złożony przez powoda certyfikat systemu A.. Wynika bowiem z niego, że dotyczy on trzech komputerów funkcjonujących w przedsiębiorstwie powoda, a w toku postępowania ostatecznie nie udało się ustalić, czy certyfikat ten obejmował wszystkie komputery w tym przedsiębiorstwie, a przede wszystkim – czy obejmował on ten komputer, na którym skarżący w dniu 11 maja 2015 roku próbował się logować do systemu pozwanego banku. Tym samym nawet jeżeli podzielić by uwagę biegłego, że skoro powód miał licencję oprogramowania antywirusowego, to brak jest podstaw do przyjęcia, że tego oprogramowania nie zainstalował, to jednak nadal brak jest dowodu, że to właśnie komputer używany w dniu 11 maja 2015 roku chroniony był tym oprogramowaniem. Jednoznaczne wyjaśnienie tej kwestii dałoby badanie dysku powyższego urządzenia przez biegłego, zwłaszcza że jeszcze na rozprawie przed Sądem I instancji w dniu 11 marca 2016 roku powód deklarował złożenie tego dysku jako dowodu w sprawie, jednak już na rozprawie w dniu 27 kwietnia 2016 roku S. L. wskazał, że dysk zaginął, co w efekcie uniemożliwiło w zasadzie ustalenie zarówno wspominanej wyżej kwestii prawidłowego zabezpieczenia komputera, jak i okoliczności przeprowadzenia nań ataku hakerskiego. Powód przyznał natomiast wprost, że tego urządzenia nie zabezpieczył hasłem, wskutek czego miały do niego swobodny dostęp inne osoby, w tym przede wszystkim pracownicy powoda, co nawiasem mówiąc również stanowiło naruszenie Regulaminu świadczenia usług bankowości elektronicznej, którego powód zobowiązał się przestrzegać.

W ocenie Sądu Okręgowego wszystkie okoliczności faktyczne rozpoznawanej sprawy wskazują w sposób niebudzący wątpliwości, że to od powoda sprawca ataku hakerskiego z dnia 11 maja 2015 roku uzyskał wszelkie dane, w tym hasło umożliwiające logowanie do systemu banku oraz kod autoryzacji zlecenia płatniczego (przelewu), przy czym właśnie sposób uzyskania przez wspomnianego sprawcę kodu niezbędnego do zatwierdzenia transakcji – a zatem sposób uzyskania instrumentu płatniczego – pozostawał zdecydowanie najistotniejszy dla oceny wypełnienia przez powoda obowiązków określonych w art. 42 ustawy. S. L. twierdził, że podał kod przy przelewie, przy czym dokonując przelewu musiał podać dwa kolejne kody – pierwszy kod został wskazany jako wadliwy, a dopiero po podaniu drugiego udało mu się skutecznie dokonać transakcji. W ocenie Sądu Okręgowego należy jednak zauważyć, że pozwany przedłożył dokładne informacje – z precyzyjnym podaniem godziny – o logowaniu przez powoda do serwisu internetowego (...) /k. 171 – 172/, a także dokument przedstawiony jako wyciąg z logu systemowego /k. 183 – 183v/. Z dowodów tych, niekwestionowanych przez powodów na żadnym etapie sprawy, wynika, że pierwsze logowanie w dniu 11 maja 2015 roku miało miejsce o 10.48, drugie zaś – o godz. 10.54, przy czym po żadnym z powyższych logowań powód nie wykonywał przelewów. Pierwszy przelew został bowiem zlecony dopiero później, tj. o godzinie 11.05. Co zaś istotne, podczas rozmowy telefonicznej z pracownikiem pozwanego banku (...) o godz. 10.54 powód mówił wprawdzie o problemach z logowaniem do serwisu internetowego (przełączaniu go ze starej strony serwisu na nową), ale ani w tej, ani w kolejnej rozmowie nie poinformował pracownika banku o próbach dokonania przelewu bądź o podaniu kodu. Również z informacji podawanych przez niego w toku niniejszego postępowania wynika, że przed pierwszą rozmową (z E. N.) nie dokonywał przelewu. Tym samym w ocenie Sądu Okręgowego nie ulega wątpliwości, że przed godziną 10.54 powód nie powinien był używać instrumentu płatniczego w postaci kodu do zatwierdzenia transakcji, bowiem nic nie wskazywało na potrzebę użycia takiego kodu. Tymczasem ze wspomnianego wyżej wyciągu z logu systemowego jednoznacznie wynika, że zmiana numeru rachunku bankowego przez sprawcę ataku hakerskiego, tj. utworzenie przez niego nowego szablon odbiorcy (numer rachunku z: (...), numer rachunku na: (...), nazwa odbiorcy: D. K., tytułu płatności: (...)) nastąpiło właśnie o godzinie 10.54 i było autoryzowane kodem nr (...) z karty kodów znajdującej się w wyłącznej dyspozycji skarżącego. Innymi słowy, zestawienie czasu dokonania poszczególnych czynności – powoda i sprawcę ataku hakerskiego – wynikające z dowodu w postaci wyciągu z logu systemowego nie pozostawia w ocenie Sądu Okręgowego wątpliwości, że powód podał kod z posiadanej karty kodów przed godziną 10.54, a zatem jeszcze przed rozpoczęciem wykonywania przelewów. Biorąc zaś pod uwagę fakt, że – jak już wspomniano – tylko powód dysponował kartą kodów, o godz. 10.54 nie wykonywał on jeszcze przelewu,

a żądanie podania kodu nr (...) nie pochodziło od banku, oczywiste jest, że S. L. sam podał ten kod sprawcy ataku hakerskiego, choć nic nie wskazywało na konieczność tego typu działania. Jednocześnie nie ulega też wątpliwości, że o użyciu kodu w powyższych okolicznościach nie poinformował on pozwanego dzwoniąc doń po raz pierwszy, a trudno nie zgodzić się z Sądem I instancji, że gdyby bank uzyskał taką wiadomość już o 10.54, podjąłby standardowe kroki, które dokładnie opisała świadek J. G., tj. zaleciłby zmianę hasła dostępu, „oczyszczenie" komputera oraz sprawdzenie historii operacji na swoim rachunku, co zdecydowanie zredukowałoby prawdopodobieństwo udanego ataku hakerskiego. W rozmowie z E. N. powód powiedział tymczasem, że przed 10.54 nie logował się do swego konta /k. 134/. Analogiczne stwierdzenie padło też z ust świadek E. N., która wskazała, że powód w rozmowie z nią mówił jedynie o braku możliwości zalogowania się do serwisu internetowego, a informacje od niego nie wskazywały na jakiekolwiek nieprawidłowości. Także druga rozmowa powoda z pracownikiem banku miała podobny przebieg i dotyczyła braku możliwości zalogowania i odsyłania powoda na inną stronę. W ocenie Sądu Okręgowego takie informacje podawane przez powoda nie były – wbrew jego twierdzeniom – podstawą do zablokowania konta, bowiem tego typu czynności mogą być podęte wyłącznie w usprawiedliwionych okolicznościami sytuacjach, a bank nie może dowolnie blokować konta swego klienta. Mimo zatem tego, że powód zarówno w rozmowach z pracownikami pozwanego, jak i w toku niniejszego postępowania konsekwentnie twierdził, że używał kodów tylko przy zatwierdzaniu transakcji, zdaniem Sądu Okręgowego nie ulegało wątpliwości, że zanim zalogował się on do serwisu (...) i rozpoczął przelewy, sprawca atak hakerskiego już dysponował kodem do zatwierdzenia transakcji, służącym mu w celu utworzenia szablonu nowego odbiorcy. Kod ten został mu zaś udostępniony przez powoda, który podał go mimo widniejących na stronie banku ostrzeżeń, że służy on wyłącznie do autoryzacji zleconej w serwisie dyspozycji. Powód udostępnił zaś instrument płatniczy w okolicznościach innych, niż autoryzacja zleconej w serwisie dyspozycji. W konsekwencji nie tylko nie wypełnił on obowiązku nieudostępniania instrumentu płatniczego osobom nieuprawnionym (art. 42 ust. 2 ustawy), ale nie mówiąc o fakcie takiego udostępnienia już w pierwszej rozmowie z pracownikiem banku nie wypełnił on też innego obowiązku – zgłaszania dostawcy stwierdzenia nieuprawnionego dostępu do instrumentu płatniczego w postaci kodu nr (...) z karty kodów (art. 42 ust. 1 pkt 2 ustawy). Brak hasła dostępu do komputera i aktualnego oprogramowania antywirusowego oznaczał zaś złamanie umowy ramowej z bankiem i niewypełnienie obowiązku przewidzianego w art. 42 ust. 1 pkt 1 ustawy. W świetle powyższych okoliczności trudno było nie ocenić zachowania powoda jako rażącego niedbalstwa w rozumieniu art. 46 ust. 3 ustawy, wskazującego na jego odpowiedzialność za nieautoryzowane transakcje płatnicze w pełnej wysokości, co istotnie – jak prawidłowo uznał Sąd Rejonowy – uzasadniało oddalenie powództwa w niniejszej sprawie w całości.

Reasumując należy stwierdzić, iż Sąd I instancji wydał trafne rozstrzygnięcie na podstawie wszechstronnej oceny zebranego w sprawie materiału dowodowego, a odmienne twierdzenia apelacji powodów, dotyczące zarówno naruszenia przepisów prawa materialnego, jak i procesowego, nie mogły zyskać aprobaty.

Mając powyższe na uwadze należało orzec na podstawie art. 385 kpc jak w pkt. I sentencji.

O kosztach postępowania odwoławczego Sąd Okręgowy orzekł na podstawie art. 98 kpc i zawartej w niej zasady odpowiedzialności za wynik procesu ustalając koszty zastępstwa procesowego pozwanego na kwotę 2.700 zł, zgodnie z § 2 pkt 6 w zw. z § 10 ust. 1 pkt 1 rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 roku w sprawie opłat za czynności radców prawnych (Dz. U. 2015, poz. 1804).