Sygn. akt XVI C 169/16

UZASADNIENIE

W pozwie z dnia 8 stycznia 2016 r. (data nadania w placówce pocztowej) powódka D. I. wniosła o zasądzenie od strony pozwanej (...) Bank (...) S.A. z siedzibą w W. (dalej także jako: Bank, (...) S.A.") na jej rzecz kwot 44 321,97 zł, 15 zł oraz 465,86 zł z odsetkami ustawowymi za opóźnienie naliczanymi od dat szczegółowo określonych w pozwie oraz kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych i kosztów opłaty skarbowej od pełnomocnictw.

W uzasadnieniu wskazano, że (...) S.A. prowadzi dwa rachunki bankowe na rzecz powódki, z których w dniu 26 maja 2015 r. bez zlecenia, wiedzy i zgody powódki dokonano przelewów pomiędzy rachunkami własnymi powódki oraz ostatecznie trzech przelewów na rachunek, który według opisu z potwierdzeń przelewów należy do J. J.. Łączna kwota przelewów wyniosła 44 178 zł. Razem z naliczonymi opłatami suma uszczuplenia wyniosła 44 321,97 zł.

Powódka niezwłocznie zawiadomiła o tym fakcie Bank oraz Policję. Bank nie uwzględnił reklamacji powódki. W piśmie z 31 lipca 2015 r. stwierdził, że opisane transakcji zostały zlecone po poprawnym zalogowaniu się w serwisie (...) numerem powódki oraz jej hasłem dostępu. Powódka nie podawała nikomu tych danych i nie wie, w jaki sposób nieuprawnione osoby znalazły się w ich posiadaniu. Bank wskazał, że do realizacji tych transakcji doszło „w wyniku zainfekowania stacji roboczej", z której powódka logowała się do serwisu (...), złośliwym oprogramowaniem oraz że wirus spowodował, że po zalogowaniu powódka otrzymała fałszywy komunikat z prośbą o podanie kodu autoryzacyjnego. W ten sposób osoby nieupoważnione miały zdefiniować nowy szablon płatności na podstawiony rachunek odbiorcy, który następnie został wykorzystany do realizacji przelewów. Powódka zaprzecza jednak, by taka sytuacja miała miejsce. Logowała się z komputera z zainstalowanym programem antywirusowym. Zawsze postępowała zgodnie z Regulaminem świadczenia usług bankowości elektronicznej i nie spotkała się z żadną nietypową sytuacją. Powołała się na nienależyte wykonanie umowy rachunku bankowego przez Bank, a nadto na treść art. 42, art. 43 oraz art. 46 ustawy o usługach płatniczych z dnia 19 sierpnia 2011 r. (Dz.U. Nr 199, poz. 1175 ze zm.; dalej: u.u.p.).

Powódka wskazała kolejno, że wskutek dokonania nieautoryzowanych transakcji powstał debet. Powódka została z tego tytułu obciążona kosztami z nim związanymi w kwotach 15 zł (za zawiadomienie) oraz 465,86 zł (tytułem odsetek) (pozew – k. 1-7).

W odpowiedzi na pozew strona pozwana wniosła o oddalenie powództwa w całości jako bezzasadnego i zasądzenia od powódki kosztów postępowania, w tym kosztów zastępstwa procesowego według norm przepisanych.

W uzasadnieniu wskazano, że przy dokonywaniu spornych transakcji na rachunku powódki nie doszło do złamania zabezpieczeń systemów bankowych, zalogowanie nastąpiło z podaniem prawidłowego loginu powódki, zaś same transakcje zostały zrealizowane w oparciu o szablon płatności prawidłowo aktywowany przy pomocy jednorazowego kodu aktywacyjnego przekazanego drogą wiadomości SMS na numer telefon powódki. Nie można wobec tego mówić w niniejszej sprawie o nieautoryzowanej transakcji w rozumieniu art. 40 u.u.p. W niniejszej sprawie albo powódka świadomie utworzyła szablon płatności dla odbiorcy zdefiniowanego jako J. J. albo nastąpiło naruszenie przez powódkę zasad bezpieczeństwa posługiwania się bankowością elektroniczną, bądź poprzez zamierzone udostępnienie instrumentów weryfikacyjnych i autoryzacyjnych osobie trzeciej, bądź w wyniku naruszenia innych zasad bezpieczeństwa. W szczególności może chodzić o naruszenie obowiązku stosowania legalnego, aktualnego oprogramowania antywirusowego oraz zapory firewall, a także najnowszych wersji przeglądarek oraz zachowanie szczególnej uwagi przy korzystaniu ze stron podobnych do stron Banku. Dokonując analizy dostępnych informacji można jedynie przypuszczać, że realizacja transakcji nastąpiła w wyniku zainfekowania tzw. złośliwym oprogramowaniem stacji roboczej, z której powódka logowała się do serwisu (...). O ile powódka nie działała świadomie, to nie zabezpieczyła ona używanego urządzenia w sposób wymagany do uniknięcia zainfekowania wirusem, a także nie zachowała należytej ostrożności w sytuacji żądania od niej czynności nietypowej, polegającej

na podaniu jednorazowego kodu aktywacyjnego w sytuacji, gdy była ona wielokrotnie informowana o tym, że Bank nigdy nie żąda podania tych kodów podczas logowania. Z wyciągu z systemu bankowego wynika, że kod SMS został wysłany na numer telefonu powódki w dniu 25 maja 2015 r. o godz. 15:20. Przy użyciu podanego przez powódkę kodu autoryzacyjnego na jednym z rachunków powódki został zdefiniowany nowy szablon płatności, który został następnie wykorzystany przez nieznanego sprawcę do realizacji na jego podstawie przelewów zakwestionowanych przez powódkę. Do przeprowadzenia wszystkich operacji wystarczyło jednokrotne wprowadzenie kodu.

Strona pozwana podniosła również, że powódka nie wykazała odpowiedzialności strony pozwanej za wypłatę środków z jej rachunku bankowego. W ocenie Banku brak jest podstaw do przypisania mu odpowiedzialności odszkodowawczej w reżimie odpowiedzialności deliktowej (odpowiedź na pozew – k. 51-73).

W replice na odpowiedź na pozew z 13 maja 2016 r. (data nadania przesyłki w placówce pocztowej) strona powodowa zaprzeczyła twierdzeniom banku. W szczególności wykluczyła, by mogło mieć miejsce „zainfekowanie" jej komputera. Podkreśliła, że do logowania się używała tylko dwóch komputerów, co odzwierciedlają odpowiednie numery IP, wynikające z wydruków z systemu Banku. Jedynie w dniu dokonania nieautoryzowanych transakcji, tj. 26 maja 2015 r., pojawia się nowy numer IP. Zdaniem powódki, okoliczność ta potwierdza, że pozwany dopuścił do wejścia w posiadanie przez osoby nieuprawnione danych, które umożliwiły im zalogowanie się na konto powódki. Nie dochował więc wymogu należytej staranności. Powódka podkreśliła, że komputery z których logowała się do (...) były prawidłowo zabezpieczone, zgodnie z wymogami strony pozwanej. Odpowiedzialność za spowodowanie szkody powódka opiera na reżimie odpowiedzialności kontraktowej (nie wykluczając deliktu)(replika – 128-141).

W dalszym toku postępowania strony podtrzymały swoje stanowiska w sprawie.

Sąd ustalił następujący stan faktyczny:

W dniu 13 lutego 2013 r. D. I. zawarła z (...) S.A. umowę o prowadzenie rachunku oszczędnościowo-rozliczeniowego (...) bez G., usług bankowości elektronicznej oraz karty debetowej (bez (...)). Na mocy tej umowy (...) S.A. zobowiązał się do prowadzenia rachunku oszczędnościowo – rozliczeniowego (...) bez G. w walucie polskiej o numerze (...), na zasadach określonych w umowie i Regulaminie rachunku oszczędnościowo-rozliczeniowego, usług bankowości elektronicznej oraz karty debetowej w (...) S.A. (§ 1 umowy). Zgodnie z § 9 ust. 2 umowy realizacji dyspozycji składanych za pośrednictwem bankowości elektronicznej (...) odbywa się z uwzględnieniem Regulaminu.

(***dowód*** : umowa – k. 14-18)

W dniu 15 lutego 2013 r. D. I. zawarła z (...) S.A. umowę o prowadzenie rachunku oszczędnościowego oraz świadczenie usług bankowości elektronicznej. Na mocy tej umowy (...) S.A. zobowiązał się do prowadzenia rachunku oszczędnościowego, potwierdzenia otwarcia rachunku oraz świadczenia usług bankowości elektronicznej (§1 umowy). Integralną część umowy stanowiło potwierdzenia otwarcia w dniu 15 lutego 2013 r. rachunku oszczędnościowego plus o numerze (...).

(***dowód*** : umowa – k. 21-24, potwierdzenie otwarcia rachunku – k. 25-26)

Zgodnie z Regulaminem świadczenia usług bankowości elektronicznej w (...) Banku (...) S.A. klient zobowiązany był do logowania oraz wykonywania dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście z użyciem instrumentów uwierzytelniających. Poza tym klient zobowiązany był do zachowania w tajemnicy informacji zapewniających bezpieczne korzystanie z usługi bankowości elektronicznej, w tym informacji przekazanych (...) Bankowi (...) S.A. dla celów weryfikacji oraz nieudostępniania i nieujawniania innym osobom instrumentów uwierzytelniających. Klient zobowiązany był do należytego zabezpieczenia urządzeń i oprogramowania (...) którymi posługuje się w celu korzystania z usług bankowości elektronicznej poprzez stosowanie: wyłącznie legalnego oprogramowania, jego bieżącą aktualizację, i instalację poprawek systemowych zgodnie z zaleceniami producentów, aktualnego oprogramowania antywirusowego i antyspamowego oraz zapory firewall, najnowszych wersji przeglądarek internetowych, haseł zabezpieczających przed nieuprawnionym dostępem do komputera osób

trzecich. Szczegółowy opis środków, jakie powinien przedsięwziąć klient w celu zapewnienia bezpieczeństwa dostępu do usług bankowości elektronicznej podawany jest do wiadomości klientów i użytkowników na stronie internetowej, oraz w serwisie telefonicznym (§ 12 ust. 1 – 4 Regulaminu).

(...) Bank (...) S.A. rozpatruje reklamacje niezwłocznie, w terminie nie dłuższymi niż 30 dni. W przypadku braku możliwości rozpatrzenia reklamacji w tym terminie, (...) Bank (...) S.A. poinformuje klienta o planowanym terminie udzielenia odpowiedzi (§ 20 ust. 7 Regulaminu).

(***okoliczności bezsporne, a nadto:*** Regulamin świadczenia usług bankowości elektronicznej w (...) Banku (...) S.A.– k. 87 – 89v)

D. I. jako posiadacz ww. rachunków bankowych korzystała z usług bankowości elektronicznej poprzez serwis internetowy (...). Do autoryzacji wszelkich wymagających tego operacji wykonywanych za pośrednictwem Internetu wymagane było podanie nadanego jej loginu i hasła. Dalsza weryfikacja następowała na podstawie jednorazowych kodów wysyłanych przez Bank w wiadomości SMS na jej numer telefonu po ich wpisaniu do systemu. W bankowości internetowej możliwe było zdefiniowanie odbiorcy. Usługa ta była dedykowana dla sytuacji, gdy właściciel rachunku bankowego zamierzał na rzecz konkretnej osoby dokonywać wielu przelewów. Dla zdefiniowania stałego odbiorcy konieczne było utworzenie szablonu i jego autoryzowanie kodem sms otrzymanym z Banku. Po utworzeniu szablonu, dokonywanie płatności na ten rachunek możliwe było już bez konieczności wpisywania dalszych kodów autoryzacyjnych otrzymywanych sms-em.

(***okoliczności bezsporne, a nadto:*** zeznania świadka J. G. – czas nagrania 00:09:28 – 00:18:39 – k. 242 – 243)

W okresie od kwietnia do końca maja 2015 roku D. I. korzystała z bankowości internetowej logując się do niej jedynie z dwóch nr (...)(numer przypisany do komputera domowego D. I.) oraz (...)(numer przypisany do miejsca pracy (...) S.A.)

(dowód: wydruk logowań z numerami IP – k. 99 – 100, informacja – k. 202, zeznania powódki – czas nagrania 00:53:43 – 00:54:50 – k. 431).

Komputer w miejscu pracy powódki (nr(...)) był zabezpieczony oprogramowaniem antywirusowym, dwoma warstwami firewall oraz systemami automatycznego wykrywania i blokowania ataków z zewnątrz na infrastrukturę (...). Dnia 26 maja 2015 roku na skrzynki pracowników (...) została skierowana akcja phishingowa, otrzymali podejrzane maile które wyglądały jak maile od kuriera (...). Pracownicy zgłosili te informacje, w tym D. I., służbom informatycznym. Wówczas komputer powódki został wyłączony i wyczyszczony, usunięto z niego wszelkie dane.

(***dowód:*** zeznania świadka J. J. – czas nagrania 00:11:09 – 00:18:48 – k. 219).

Najpóźniej w dniu 25 maja 2015 r. nieznana osoba lub osoby uzyskały login i hasło umożliwiające zalogowanie się na konto D. I. w serwisie internetowym (...). W dniu 25 maja 2015 r. na numer telefonu D. I. został wysłany przez Bank wiadomość SMS z jednorazowym kodem autoryzacyjnym. Treści tego smsa brak w historii telefonu, którym wówczas D. I. się posługiwała. Podczas sesji trwającej w dniu 25 maja 2019 r. od godziny 15:19:14 do 15:21:53 utworzono szablon płatności dla odbiorcy zdefiniowanego jako J. J., który został uwierzytelniony za pomocą wysłanego przez Bank kodu sms na numer telefonu D. I.. Ta sesja została nawiązana z (...)(przypisany do służbowego komputera D. I. w (...)).

(***dowód*** : zeznania świadka J. G. – czas nagrania 00:27:56 – 00:28:56 – k. 243v; częściowo opinia biegłego P. J. – k. 229, wyciąg z systemu bankowego rejestrującego kody uwierzytelniające – k. 63, informacja – k. 33, umowa – k. 187 – 190, opinia biegłego A. N. – k. 363 – 369v, opinia uzupełniająca k. 395 – 398)

W dniu 26 maja 2015 r. nieznany sprawca lub sprawcy skutecznie dwukrotnie zalogowali się (adres (...)– przypisany do Z. T.) na konto w bankowości internetowej D. I. (nr (...)). Po raz pierwszy o godzinie 9:49 i po raz drugi o godzinie 10:52. Logowanie nastąpiło z adresu IP przypisanego do mieszkania we W.. Wcześniej mieszkanie to wynajmowała

P. T., na której prośbę właścicielka mieszkania zawarła umowę z (...) S.A. o dostawę usług internetowych. Umowa ta została rozwiązana we wrześniu 2015 roku.

(***dowód*** : monitor logowań klientów (...)/ (...) k. 99-100, raport danych retencyjnych – k. 200 – 201, zeznania świadka P. T. – czas 00:08:19 – 00:14:52 - k. 307).

Sprawca lub sprawcy zlecili wykonanie trzech przelewów z rachunku oszczędnościowo – rozliczeniowego D. I. o numerze (...) na rachunek wcześniej zdefiniowanego odbiorcy o numerze (...) 0000 0001 2976 (...), prowadzony dla J. J.. Przelane kwoty to kolejno 19 790 zł, 19 888 zł oraz 4 500 zł. Za wykonanie każdego z tych przelewów Bank obciążył rachunek D. I. kwotą 40 zł tytułem opłaty za przelew w systemie S.. Dokonanie przelewów na rachunek nr (...) 0000 0001 2976 (...) poprzedzone było przelewami z rachunku oszczędnościowego D. I. nr (...) na rachunek oszczędnościowo – rozliczeniowy D. I. nr (...) w kwotach 19 790 zł, 5 000 zł, 3 000 zł. Za te transakcje obciążono rachunek D. I. nr (...) każdorazowo kwotą 7,99 zł tytułem „opłata –przelew wewn. dowolny".

Ze względu na to, że odbiorcą przelewu był odbiorca zdefiniowany w szablonie płatności, do realizacji przelewu nie było wymagane potwierdzenie poprzez wprowadzenie kodu wysłanego przez Bank na telefon D. I..

(***dowód:*** zestawienie operacji – k. 30 – 31, 32 – 33, informacja – k. 33).

D. I. ani P. T. nigdy nie słyszały o osobie takiej jak J. J.. Z ustaleń poczynionych w ramach prowadzonego postępowania przygotowawczego przez policję, paszport którym miał posługiwać się J. J. przy zakładaniu rachunku bankowego na który zostały przelane środki D. I., został zgłoszony jako zagubiony 14 kwietnia 2015 roku.

(dowód: zeznania powódki – 00:50:06 – 00:50:19 – k. 430, zeznania świadka P. T. – czas 00:11:52 – 00:12:51 - k. 307, postanowienie – k. 381 – 383).

Kolejno Bank obciążył rachunek bankowy prowadzony dla D. I. nr (...) w okresie od czerwca do listopada 2015 roku łącznie kwotą 465,86 zł tytułem „kapitalizacja odsetek-obciążenie", które to odsetki pobierane były od wykazywanego na tym rachunku debetu. Dnia 17 lipca 2015 roku rachunek ten obciążono także kwotą 15 zł tytułem opłaty od zawiadomienia o nieterminowej spłacie.

(***dowód:*** zestawienie operacji – k. 34 – 37v).

D. I. dnia 26 maja 2015 roku, po przyjściu do pracy o godzinie 13:00, logując się na konto (...) o godzinie 13:02 zauważyła dokonanie nieautoryzowanych przelewów i zgłosiła ten fakt Bankowi oraz bankowi beneficjenta przelewu (...). Zgłosiła także reklamację na infolinię.

(***dowód:*** monitor logowań klientów (...)/ (...) k. 99-100, zgłoszenie – k. 38, odtworzenie nagrania – k. 148, płyta CD – k. 124, zeznania powódki D. I. – czas nagrania 00:42:37 – 00:50:06 – k. 429 - 430)

Tego samego dnia złożyła na Komendzie Rejonowej Policji W. I ustne zawiadomienie o podejrzeniu popełnienia przestępstwa polegające na dokonaniu nieuprawnionych przelewów.

(***dowód*** : pismo z Policji – k. 43)

Na skutek złożenia zawiadomienia wszczęte zostało dochodzenie w sprawie czynu z art. 286 § 1 k.k. Postępowanie to zostało umorzone ze względu na niewykrycie sprawcy.

(***okoliczności bezsporne, a nadto:*** zawiadomienie – k. 44, dokumenty z akt postępowania przygotowawczego – k. 182-206, postanowienie – k. 381- 383).

W piśmie z dnia 17 czerwca 2015 roku Bank poinformował D. I., że jej reklamacja jest przedmiotem dalszej analizy, a czas jej rozpoznania może być wydłużony.

W kolejnym piśmie z dnia 31 lipca 2015 roku Bank odmówił uwzględnienia reklamacji na podstawie art. 46 ust. 3 u.u.p. Analiza dokonana przez Bank wykazała, że transakcje zostały zlecone po poprawnym zalogowaniu w serwisie (...) numerem klienta i hasłem dostępu D. I.. Wskazał, że ich realizacja nastąpiła w wyniku zainfekowania stacji roboczej, z której D. I. logowała się do serwisu (...), złośliwym oprogramowaniem.

(***okoliczności bezsporne, a nadto:*** pisma Banku – k. 40-42)

Od lutego 2015 roku (data na ostatniej stronie wydruku) dostępny był dla klientów Banku (...) po usługach bankowości elektronicznej (...). Przewodnik ten zawierał ogólne informacje o sposobie korzystania z bankowości internetowej. W części (...) wskazano by nigdy nie udostępniać hasła i numeru klienta osobom trzecim i nie podawać ich na nieszyfrowanych stronach (czyli takich, na których nie ma zainstalowanego certyfikatu bezpieczeństwa danej strony. Certyfikat można sprawdzić klikając w ikonę „kłódki"). Zalecono również upewnienie się czy system W. posiada najnowsze uaktualnienia oraz stosowanie najnowszych wersji przeglądarek internetowych oraz prowadzenie ich okresowej aktualizacji.

(***dowód:*** P. po usługach – k. 107 – 121).

Dopiero dnia 19 czerwca 2015 roku na stronie internetowej Banku pojawił się komunikat: „fałszywe komunikaty – nie otwieraj załączników".

(***dowód***: zrzut z ekranu – k. 92).

Przed przedmiotowym zdarzeniem Bank monitorował dokonywane transakcje, starając się identyfikować operacje podejrzane, nietypowe. Stosował parametry, które w wypadku ich zaistnienia kwalifikowały daną operację do dodatkowego potwierdzenia. Wyżej opisane transakcje nie zostały zaalarmowane jako podejrzane. Po masowej akcji hakerskiej na banki w 2015 roku, gdzie posługiwano się mechanizmem tworzenia szablonów zaufanego odbiorcy, parametry te zostały zmienione. W wyniku powyższego, transakcje polegające na stworzeniu szablonu płatności zaufanego odbiorcy i potem wykonywaniu kilku przelewów na podstawie tych szablonów, najprawdopodobniej zostałyby wyłapane.

(***dowód***: zeznania świadka J. G. – czas nagrania 00:22:10 – 00:26:52 – k. 243 – 243v)

Dnia 26 maja 2015 roku średni kurs NBP euro wynosił 4,1279 zł.

(***okoliczność powszechnie wiadoma***, zamieszczona na stronach internetowych NBP – wydruk – k. 485).

Odpis pozwu został doręczony Bankowi dnia 4 marca 2016 roku.

Dowód: potwierdzenie doręczenia – k. 486.

Powyższy stan faktyczny Sąd ustalił na podstawie powołanych wyżej dokumentów, uznając, że nie było podstaw, by podawać w wątpliwość okoliczności faktyczne wynikające z ich treści. Sąd uznał, że dowody z tych dokumentów tworzą spójny, nie budzący wątpliwości w świetle wskazań wiedzy i doświadczenia życiowego, a przez to w pełni zasługujący na wiarę materiał dowodowy. Czyniąc ustalenia faktyczne, Sąd uwzględnił także zgodne twierdzenia stron w trybie art. 229 k.p.c. oraz twierdzenia strony, którym przeciwnik nie przeczył w trybie art. 230 k.p.c.

Jako za w całości wiarygodne Sąd uznał zeznania przesłuchanych w sprawie świadków J. J. (pracownika informatycznego (...) w którym powódka pracuje), J. G. (specjalistki w zespole monitoringu i autoryzacji operacji w pozwanym Banku) oraz P. T. (inicjatorki zawarcia umowy abonamentowej, w oparciu o którą przydzielono IP z którego wykonano polecenie wypłaty środków z rachunku powódki). Były to bowiem osoby w żaden sposób niezainteresowane rozstrzygnięciem w tej sprawie. Ich zeznania były przy tym jasne i logiczne oraz korespondowały z pozostałym materiałem dowodowym zgormadzonym w aktach sprawy. Nadto nie były kwestionowane przez strony postępowania.

Ponadto Sąd, w celu ustalenia okoliczności, w jakich doszło do dokonania nieautoryzowanych transakcji, dopuścił dowód z opinii biegłego z informatyki i telekomunikacji.

Opinia biegłego P. J. pozostawała przydatna dla rozstrzygnięcia jedynie w zakresie w jakim wykonał on swój obowiązek, tj. zbadał telefon będący w posiadaniu pozwanej na który miała przyjść dnia 25 maja 2015 roku wiadomość autoryzująca utworzenie szablonu i stwierdził, że w historii tego telefonu wiadomości tej nie ma. W pozostałym zakresie Sąd uznał tę opinię za całkowicie nieprzydatną, jako nie zawierającą ustaleń opartych na wiedzy specjalnej, a jedynie prawne oceny biegłego, wykraczające dalece poza jego kompetencje.

Wobec powyższego, konieczne stało się dopuszczenie dowodu z opinii kolejnego biegłego – A. N..

Rozważając wnioski opinii głównej, opinii pisemnej uzupełniającej i ustnej opinii uzupełniającej oraz zgłaszane pod ich adresem zarzuty stron Sąd doszedł do przekonania, że opinia biegłego A. N. stanowi pełnowartościowy materiał dowodowy, mogący służyć za podstawę dokonywania ustaleń faktycznych w sprawie. Opinia ta cechuje się fachowości, rozważania w niej zawarte są logiczne, a wnioski dokładnie uzasadnione. Brak było podstaw do kwestionowania jej poprawności. Ostatecznie jednakże opinia ta nie udzieliła odpowiedzi na pytanie, w jaki sposób doszło do nieautoryzowanych transakcji z konta powódki. Biegły przedstawił szereg hipotez, które w mniejszym lub większym stopniu odpowiadały pozostałemu materiałowi dowodowemu zgromadzonemu w aktach sprawy. Hipotezy te cechowały się w ocenie Sądu fachowością i rzetelnością w prezentowaniu wiedzy specjalnej biegłego, co jednakże nie zmienia postaci rzeczy, że opinia ta nie miała waloru pewności co do przebiegu zdarzeń.

Odnośnie danych dotyczących faktu, iż sms z kodem autoryzacyjnym został wysłany na numer telefonu powódki, Sąd uznał tę okoliczność za udowodnioną wobec pozytywnego zweryfikowania tych danych przez biegłego A. N., w oparciu o zapisy z systemu wewnętrznego Banku, przedstawione na płycie CD. Informacje te nie wynikały więc jedynie z twierdzeń strony pozwanej przedstawionych w formie zrzutu z ekranu (co kwestionowała powódka) lecz stanowiły prezentację danych z systemu informatycznego. Ich zafałszowanie wymagałoby więc ingerencji w ten system, co w ocenie Sądu biegły powinien byłby zauważyć.

W toku niniejszego postępowania nie udało się ponad wszelką wątpliwość ustalić czy sms z kodem autoryzacyjnym wysłanym przez Bank na nr telefonu powódki w istocie dotarł do adresata, czy też może został w jakiś sposób przechwycony przez osoby trzecie. Jak wynika z przeprowadzonych przez biegłego P. J. oględzin telefonu, w historii wiadomości tego smsa brak. Biegły A. N. nie wykonał ostatecznie oględzin telefonu, wskazując że w sytuacji usunięcia wiadomości jej odtworzenie może nie być możliwe (k. 397). Biegły wskazał przy tym, że w jego ocenie powódka musiała odebrać smsa skoro w oparciu o niego dokonała autoryzacji utworzeniu szablonu. Musiała więc go wpisać w systemie (...) (k. 397v). Kolejno w toku składania ustnej opinii uzupełniającej, biegły jednakże stwierdził, że nie ustalił w jaki sposób doszło do wypłaty środków z rachunku powódki (k. 427). Wskazał przy tym, że na stan dzisiejszej wiedzy nie słyszeliśmy o tym aby udało się przełamać zabezpieczenie operatorów telefonii komórkowej, by przejąć smsa (k. 428). Na kolejne pytania, odnośnie wyjaśnienia posłużenia się przy tworzeniu szablonu przelewu IP komputera służbowego powódki, biegły początkowo stwierdził, że nie może wykluczyć by ktoś inny posłużył się IP powódki, ale byłoby to bardzo utrudnione (k. 428). Kolejno jednak wyjaśnił, że żyjemy w takich czasach, że nie można ufać nawet numerowi IP (k. 428), że jego zdaniem ktoś musiał przejąć IP powódki (k. 429). Powyższe wnioski nakazują uznać, że w istocie biegły stwierdzając, że powódka musiała odebrać smsa z banku, opierał się na założeniu, że do przelewu środków doszło w wyniku ataku phishingowego, na który powódka dała się nabrać, podając na fałszywej stronie banku swój login i hasło, a następnie otrzymany z Banku sms-em jednorazowy kod autoryzacyjny. Powyższe założenie musiałoby jednakże uwzględnić fakt, że do stworzenia szablonu przelewu doszło podczas logowania się dnia 25 maja 2015 roku do (...) z IP służbowego komputera powódki. Pytany o tę okoliczność biegły stwierdził jedynie, że w jego ocenie musiało dojść do przejęcia IP powódki, ale nie ma na to dowodów, lecz jest to technologicznie możliwe (k. 429). W sytuacji w której powódka zaprzeczała jakoby gdziekolwiek, kiedykolwiek wpisywała w sposób nierozważny kod otrzymany smsem z banku, wskazując także, że nie pamięta by wówczas w ogóle jakiegokolwiek takiego podejrzanego smsa otrzymała, Sąd uznał, iż opinia biegłego nie pozwoliła jednoznacznie ustalić jak doszło do stworzenia szablonu przelewu, a w konsekwencji w jaki sposób doszło do przekazania przez powódkę sprawcom loginu i hasła powódki oraz

kodu autoryzacyjnego przesłanego z Banku poprzez smsa. Przy tym jak już wcześniej wskazano, sam biegły ostatecznie przyznał, że nie ustalił w jaki sposób doszło do wypłaty środków z rachunku powódki.

Oczywiście jednym z możliwych wyjaśnień tak ustalonego ciągu zdarzeń mogłoby być przyjęcie, iż to powódka świadomie utworzyła ten szablon przelewu na rzecz osoby o danych J. J.. Okoliczność tę Sąd uznał jednakże za nieudowodnioną – o czym w dalszej części uzasadnienia.

Uznając, iż w sprawie pozostają niewyjaśnione wątpliwości, Sąd dopuścił dowód z zeznań stron, ograniczając go do powódki. Zeznania powódki Sąd uznał ostatecznie za w całości wiarygodne. Korespondowały one z pozostałym materiałem dowodowym zgormadzonym w aktach sprawy oraz nie zostały jednoznacznie podważone w opinii biegłego (w zakresie otrzymania smsa i wpisania w (...) kodu autoryzacyjnego). W szczególności wskazać tu należy na, po pierwsze, udowodnione zachowanie powódki bezpośrednio po wykryciu wypłaty środków z jej rachunku bankowego, gdzie zgłosiła tę okoliczność w pozwanym Banku oraz w banku beneficjenta przelewów oraz na policji. Po drugie, okoliczność, iż już po utworzeniu szablonu płatności, do wypłaty środków wykorzystano (...), przypisany do mieszkania we W., którego właścicielka czy najemczyni nie znały ani powódki ani beneficjenta środków. Po trzecie, rachunek bankowy beneficjenta przelewów został założony na dane osoby na podstawie paszportu, którego zagubienie wcześniej zgłoszono. Po czwarte, w okresie maja 2015 roku doszło do zorganizowanej akcji hakerskiej ataków na banki, w który to model operacyjny sprawców (posłużenie się szablonem płatności utworzonym w oparciu o jeden uzyskany kod autoryzacyjny, w celu ominięcia limitów transakcyjnych) opisywany powyżej schemat działania w stosunku do powódki się wpisuje. Mając na uwadze powyższe okoliczności Sąd uznał za wiarygodne zeznania powódki w zakresie w jakim wskazywała, że to nie ona wypłaciła środki ze swojego rachunku bankowego i nie ma ona wiedzy jak do tych transakcji doszło. Jedynie na marginesie w zakresie oceny wiarygodności zeznań powódki należy wskazać, że przyjęcie, iż nie mieliśmy tu do czynienia z atakiem hakerskim, lecz z uwagi na dane IP komputera z którego korzystano podczas sesji gdzie utworzono szablon przelewu, z działaniem samej powódki, zgodnie ze wskazaniami doświadczenia życiowego, strona pozwana powinna przedstawić takie twierdzenia także w ramach toczącego się postępowania przygotowawczego w przedmiocie przestępstwa z art. 286 § 1 k.k. Do takiego zgłoszenia, czy przedstawienia takich wątpliwości przez Bank, jednakże nie doszło.

Odnosząc się jeszcze w tym miejscu do kwestii oddalonego wniosku o przeprowadzenie w trybie zabezpieczenia dowodu z oględzin rzeczy (k. 54 w zw. z k. 125), wyjaśnić należy, iż Sąd nie uznał, by przeprowadzenie tego dowodu w trybie zabezpieczenia było niezbędne. Po pierwsze, wniosek o zabezpieczenie dowodu nie został w żaden sposób uzasadniony. Po drugie, został zgłoszony w odpowiedzi na pozew, doręczonej bezpośrednio pełnomocnikowi powódki. Powódka miała więc o nim wiedzę, zanim Sąd zdążyłby go rozpoznać. Gdyby więc zamierzała usunąć jakiekolwiek niewygodne dla niej dane, mogłaby to uczynić, zanim termin oględzin z udziałem biegłego by nadszedł. Po trzecie, wniosek ten pozostawał nieprecyzyjny. W oparciu o same twierdzenia odpowiedzi na pozew i załączone do niej dokumenty (nr IP) nie sposób było ustalić skąd następowało logowanie do bankowości internetowej, a w konsekwencji gdzie są położone komputery z których powódka miała korzystać (okoliczność ta została wyjaśniona na dalszym etapie postępowania). Po czwarte, niemożliwe do wykonania było zrealizowanie wniosku dowodowego o dokonanie oględzin „innych urządzeń elektronicznych", jako nieprecyzyjne.

W oparciu o powyższe ustalenia faktyczne, Sąd zważył, co następuje:

Powództwo zasługiwało w większej części na uwzględnienie.

Zgodnie z treścią art. 725 k.c. przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych. Obowiązek zachowania szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych, nakłada dodatkowo na Bank art. 50 § 2 Prawa bankowego (Dz.U. Nr 140, poz. 939 ze zm.).

W tym miejscu wyjaśnić wypada, że zawarcie umowy rachunku bankowego powoduje, że środki pieniężne posiadacza przechodzą na własność banku. Mimo braku jednoznacznego sformułowania w odnośnych przepisach ustawy, w

doktrynie i w orzecznictwie powszechny i w zasadzie niekontrowersyjny jest pogląd, że bank uzyskuje własność deponowanych pieniędzy (E. Niezbecka, [w:] Kodeks Cywilny. Komentarz. Tom III, red. A. Kidyba, Warszawa 2014, s 704-705; Z. Ofiarski, Prawo bankowe. Komentarz, Warszawa 2013, s. 384; wyrok Sądu Najwyższego z 13 lutego 2004 r., sygn. akt IV CK 40/03, Legalis nr 66917; wyrok Sądu Apelacyjnego w Krakowie z 5 lutego 2014 r., sygn. akt I ACa 917/12, Legalis nr 1093113; wyrok Sądu Apelacyjnego w Poznaniu z 27 października 2010 r., sygn. akt I ACa 733/10, Legalis nr 270878). Zgodnie z treścią art. 726 k.c. bank może obracać czasowo wolne środki pieniężne zgromadzone na rachunku bankowym z obowiązkiem ich zwrotu w całości lub w części na każde żądanie, chyba że umowa uzależnia obowiązek zwrotu od wypowiedzenia. Wynikające z umowy uprawnienie posiadacza rachunku stanowi wierzytelność do banku każdocześnie wymagalną, a jej rozmiary wskazuje stan konta. Z chwilą realizacji wierzytelności, przez zwrot środków pieniężnych, posiadacz rachunku odzyskuje ich posiadanie i także własność, bądź inne prawo rzeczowe lub obligacyjne, które było z nimi związane przed zdeponowaniem.

Reasumując, mimo wyłudzenia przez osobę nieuprawnioną mienia stanowiącego własność banku, nie dojdzie do powstania szkody po stronie posiadacza rachunku, gdyż bank nadal pozostanie zobowiązany do zaspokojenia jego wierzytelności w pełnej wysokości ze swoich środków. Ochronę wierzytelności gwarantują posiadaczowi przepisy prawa cywilnego, finansowego i oparta na nich umowa z bankiem (zob. postanowienie Sądu Najwyższego z 28 kwietnia 2016 r., sygn. akt I KZP 3/16, Legalis nr 1442847). Ze swojego długu wobec posiadacza rachunku bank nie zwolni się nawet wtedy, gdy dochowa należytej staranności przy dokonywaniu wypłaty osobie nieuprawnionej.

Podstawę dochodzonego roszczenia stanowić więc powinny co do zasady postanowienia umowy rachunku bankowego zawarte między powódką, a stroną pozwaną, wsparte wyżej przytoczonymi regulacjami ustawowymi.

Rozważając więc w pierwszej kolejności, jako podstawę żądań powódki odpowiedzialność kontraktową strony pozwanej, wynikającą z zawartej umowy rachunku bankowego, Sąd uznał, iż powódka nie zdołała udowodnić przebiegu zdarzenia powodującego szkodę ani okoliczności nienależytego wykonania zobowiązania strony pozwanej wynikającego z umowy o prowadzenie rachunku bankowego. Wobec braku wystarczających dowodów z których wynikałoby w jaki sposób doszło do posłużenia się przez osoby trzecie loginem i hasłem powódki przy logowaniu się do systemu (...), a następnie do uzyskania przez nich kodu autoryzacyjnego wysyłanego sms-em, Sąd uznał, że powódka nie udowodniła, by doszło tutaj do niewykonania lub nienależytego wykonania obowiązków przez Bank. W sprawie udowodnione zostało bowiem, że dokonując przelewów w oparciu o wcześniej utworzony szablon, posłużono się hasłem, loginem powódki oraz przesłanym jej kodem autoryzacyjnym. Powódka nie udowodniła, że doszło tu do przełamania wewnętrznych zabezpieczeń po stronie Banku.

W sytuacji, w której nie udowodniono w jaki dokładnie sposób sprawcy weszli w posiadanie powyższych danych, nie mogło być wystarczające dla przypisania odpowiedzialności stronie pozwanej za nienależyte wykonanie zobowiązania, powołanie się na zeznania świadka J. G., która opisała, że po atakach hakerskich z maja 2015 roku, doszło do zmiany algorytmów weryfikujących podejrzane transakcje oraz że w ocenie tego świadka, obecnie taka transakcja jak miała miejsce w sprawie niniejszej (z wykorzystaniem szablonu płatności) zostałaby skierowana do dodatkowej weryfikacji. Pomimo, iż świadek ta piastuje odpowiedzialne stanowisko w strukturach Banku, tych ogólnych przypuszczeń świadka, nie można uznać za wystarczające dla przyjęcia za udowodnione, że system weryfikacyjny operacji internetowych stosowany ówcześnie przez Bank był niewystarczający. Powrócić należy tu bowiem do źródła problemu, tj. brak dokładnych ustaleń co do sposobu pozyskania przez osoby trzecie newralgicznych danych powódki. W konsekwencji, skoro nie wiadomo jak do przeprowadzenia skutecznego ataku doszło, nie można postawić tezy, że zabezpieczenia Banku były niewłaściwe w stopniu uzasadniającym przyjęcie, że doszło do nienależytego wykonania zobowiązania przez Bank. Opierając się zaś o treść art. 471 k.c. w zw. z art. 725 k.c., ciężar udowodnienia tych okoliczności obciążał powódkę (art. 6 k.c.).

Mając na względzie powyższe utrudnienia w postępowaniu dowodowym dotyczącym korzystania z usług płatniczych oferowanych przez banki, ustawodawca wprowadził jednakże instrumenty dla kontrahentów banków, wynikające z przepisów ustawy o usługach płatniczych z dnia 19 sierpnia 2011 r., modyfikujące umowne regulacje stron umowy o usługi płatnicze. W niniejszej sprawie znajdowała zastosowanie wersja ustawy z dnia zdarzenia tj. 26 maja 2015 roku

(Dz.U.2014.873, tj. z dnia 2014.07.01 ze zm.). Ustawa ta była następnie ponownie nowelizowana, ale w materii tu istotnej nie zawiera przepisów przejściowych.

Zgodnie z powyższymi regulacjami wskazać więc należy, że zgodnie z art. 40 ust 1 u.u.p. transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą.

W myśl art. 42 ust. 1 u.u.p. 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. W celu spełnienia obowiązku, o którym mowa w ust. 1 pkt 1, 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).

Następnie, zgodnie z art. 45 ust. 1 u.u.p. 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. 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).

W konsekwencji, zgodnie z art. 46 u.u.p.:

1. 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.

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, jeżeli nieautoryzowana transakcja jest skutkiem:

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

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

3. 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.

4. 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.

5. Jeżeli dostawca, wbrew obowiązkowi, o którym mowa w art. 43 ust. 1 pkt 3, nie zapewnia odpowiednich środków umożliwiających dokonanie w każdym czasie zgłoszenia, o którym mowa w art. 42 ust. 1 pkt 2, płatnik nie odpowiada za nieautoryzowane transakcje płatnicze, chyba że płatnik doprowadził umyślnie do nieautoryzowanej transakcji.

Zebrany w sprawie materiał dowodowy pozwala na jednoznaczne ustalenie, iż mamy tu do czynienia z nieautoryzowanymi transakcjami. Nie może budzić bowiem wątpliwości, iż to nie powódka zleciła trzy określone

wcześniej przelewy własne z rachunku oszczędnościowego oraz trzy przelewy z rachunku oszczędnościowo – rozliczeniowego na rzecz rachunku prowadzonego na dane J. J. (według treści przelewu) w łącznej kwocie 44 178 zł. Sam fakt, iż do transakcji doszło przy posłużeniu się narzędziami autoryzacyjnymi przypisanymi do powódki, w myśli art. 45 ust. 1 i 2 nie był wystarczający. Opisane wcześniej okoliczności dotyczące zachowania powódki po spostrzeżeniu wypłaty środków, okoliczności ich wypłaty oraz informacje o trwających w tym czasie atakach hakerskich przemawiały w ocenie Sądu za uznaniem, że transakcje te nie były przez powódkę autoryzowane. Ciężar dowodu w tym zakresie spoczywał zaś na stronie pozwanej, któremu Bank nie podołał.

W następnym kroku zbadać należało więc, czy strona pozwana zdołała wykazać przesłanki zwalniające ją z obowiązku wypłaty powódce kwot przelanych w sposób nieautoryzowany, tj. czy do zdarzenia tego powódka doprowadziła umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z podstawowych jej obowiązków. Obowiązki te zostały określone w art. 42 u.u.p. i przytoczone powyżej, jak również uszczegółowione w § 12 Regulaminu.

Okoliczności sprawy pozwalają na wykluczenie tego, że powódka doprowadziła umyślnie do nastąpienia nieautoryzowanych transakcji.

Kluczowe dla rozstrzygnięcia w sprawie było więc ustalenie czy powódka doprowadziła do nich w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z jej obowiązków.

W sprawie nie zostało wykazane przez stronę pozwaną, by do przelewu środków mogło dojść w konsekwencji nie stosowania przez powódkę aktualnego oprogramowania ochronnego i antywirusowego, do czego zobowiązywał ją Regulamin. Powódka twierdziła, że jej domowy komputer jest był prawidłowo zabezpieczony programem antywirusowym i zaporą firewall. O wysoce zaawansowanych systemach zabezpieczeń na komputerze służbowym powódki (z którego to komputera miałoby dojść do utworzenia szablonu przelewu dnia 25 maja 2015 roku) zeznawał świadek odpowiadający za obsługę informatyczną w (...). Jednocześnie w zakresie wymogów dotyczących oprogramowania antywirusowego czy zapory firewall, zauważyć należy, iż ani w Regulaminie, ani w żadnym innym miejscu strona pozwana nie postawiła szczególnych wymogów w tym zakresie, wskazując jedynie, że chodzi tu o aktualne oprogramowanie czy przeglądarki internetowe. W szczególności nie ma tu mowy o wymogu korzystania z innych niż darmowe, ogólnodostępne zabezpieczenia tego typu. Niezależnie więc od okoliczności, iż w sprawie nie zostało wykazane, by powódka nie korzystała z wystarczających zabezpieczeń (wniosek o dokonanie oględzin „innych urządzeń" nie został uwzględniony w trybie zabezpieczenia dowodu, a następnie jako zwykły wniosek dowodowy został cofnięty – k. 147), wymagania w tym zakresie nie zostały postawione nadmiernie wysoko. Kolejno, nie można nie zauważyć, że jak wskazał biegły, przy przyjętym przez niego za najbardziej prawdopodobne, iż doszło tu do ataku phishingowego, oprogramowanie antywirusowe byłoby tu nieskuteczne. Ta metoda opiera się bowiem na oszukaniu ofiary w celu zalogowania się przez nią na fałszywą stronę banku.

Niewątpliwie też niezwłocznie powódka zgłosiła dostawcy nieuprawnione użycie jej instrumentu płatniczego do czego zobowiązywał ją art. 42 ust. 1 pkt 2 u.u.p.

Największe wątpliwości wiązały się natomiast z oceną, czy powódka wbrew ciążącemu na niej obowiązkowi ujawniła innym osobom numer klienta, hasło dostępu oraz kod jednorazowy (art. 12 Regulaminu) tj. czy korzystała z instrumentu płatniczego zgodnie z umową ramową (art. 42 ust. 1 pkt 1 u.u.p.). Ciężar dowodu wykazania tej okoliczności spoczywał na Banku (art. 45 ust. 2 u.u.p.).

W ocenie Sądu okoliczność ta nie została wykazana. Jak już to wcześniej wyjaśniono, na podstawie zgromadzonego w sprawie materiału dowodowego nie było możliwości dokładnego ustalenia mechaniki działania, które doprowadziło do nieautoryzowanego przelewu środków powódki. Co z tym się zaś wiąże, nie można jednoznacznie stwierdzić, by pozyskano dano powódki na skutek jej rażącego niedbalstwa.

Po pierwsze, Sąd nie uznał za wystarczająco udowodnione by do przelewu środków z rachunku bankowego powódki doszło wobec wpisania przez nią na fałszywą stronę, podszywającą się pod stronę Banku, jej loginu i hasła, a

następnie do odczytania przez nią sms-a z Banku z kodem autoryzacyjnym i wpisania go na tej fałszywej stronie. Powódka nie potrafiła jednoznacznie stwierdzić czy otrzymała tego dnia sms-a z banku z kodem autoryzacyjnym, niemniej stanowczo zaprzeczyła, by dokonywała jakichś niezamierzonych transakcji, bądź odpowiadała na zewnętrzne zapytania i je autoryzowała. Przyjęcie przy tym schematu działania przedstawionego przez biegłego jako najbardziej prawdopodobne (k. 366 – 367 i k. 428), tj. że w czasie rzeczywistym, jak powódka chciała dokonać jakiejś czynności w bankowości internetowej, w istocie podawała sprawcom swoje dane na fałszywej stronie, którzy jednocześnie logowali się na stronie (...) i zakładali szablon płatności, wymagałoby wyjaśnienia jak to możliwe, że szablon płatności został utworzony z IP komputera służbowego powódki, z którego wówczas i ona musiałaby korzystać. Biegły wyjaśniał przy tym, że zazwyczaj dochodzi w takich przypadkach do posłużenia się sfałszowanym nr IP. Z resztą do skorzystania przez sprawców ze „skradzionego" nr IP doszło dnia następnego przy dokonywaniu przelewów z rachunku powódki na konto sprawców. Biegły tego faktu wyjaśnić nie potrafił. Ostatecznie wskazał jednynie, iż musiano się tu podszyć pod numer IP, co wcześniej określał jako znacznie utrudnione, wskazując tym razem, że jest to możliwe oraz podając informację, iż hakerzy szkolą się teraz w rosyjskojęzycznych szkołach hackingu. Przede wszystkim jednakże biegły przyznał wprost, że nie ustalił w jaki sposób doszło do wyprowadzenia środków z Banku (k. 427).

Gdyby jednakże nawet przyjąć, że powódka w istocie chcąc dokonać czynności w bankowości internetowej podała na fałszywej stronie swój login i hasło, a następnie potwierdziła tę transakcję kodem otrzymanym przez sms-a, a więc naruszyła obowiązki przewidziane w art. 12 Regulaminu i art. 42 ust. 1 pkt 1 u.u.p. poprzez udostępnienie narzędzi autoryzacyjnych osobie trzeciej, to zbadać należałoby czy strona pozwana zdołała udowodnić, by do naruszenia tych obowiązków doszło wskutek rażącego niedbalstwa powódki.

W ocenie Sądu, i ta okoliczność nie została przez stronę pozwaną wykazana. Po pierwsze przypomnieć należy szerszy kontekst, iż schemat działania sprawców wpisywał się w akcję hakerskich ataków phishingowych jakie nastąpiły na banki w maju 2015 roku. Były to więc działania precyzyjne i dobrze zorganizowane. O powszechnej skuteczności tych działań świadczyć zaś muszą zeznania świadka J. G., która wprost określiła tę sytuację jako masową akcję hakerską oraz przyznała, że po niej wprowadzono zmiany w algorytmach zabezpieczeń Banku. Z powyższego wynika więc, że jeżeliby nabranie się przez powódkę na prośbę o podanie informacji przez ich wpisanie na fałszywą stronę internetową, uznać za jej rażące niedbalstwo, to konsekwentnie uznać należałoby, że wielu konsumentów których dotknęła „masowa" akcja zachowała się w sposób rażąco niedbały. Ta mnogość przypadków rażąco niedbałego zachowania się, musi zaś stawiać w wątpliwość przypisanie temu zachowania „rażącego" charakteru. Zachowanie się „rażąco niedbale" musi być bowiem w ocenie Sądu nacechowane wyjątkowością w odniesieniu do zachowania typowego, tu typowo niedbałego. Gdyby więc, przyjąć że wiele osób uległo podstępowi, to podobne zachowanie powódki nie mogłoby być już uznane za rażąco niedbałe.

Po drugie wskazać należy, iż dla oceny czy powódka zachowała się rażąco niedbale, wykazać należałoby stan świadomości powódki o zagrożeniach i fakt ich lekceważenia przez powódkę. Tymczasem z zaoferowanego stanu faktycznego wynika, że w maju 2015 roku, w zakresie stosowania zabezpieczeń czy ostrożnego postępowania w bankowości internetowej powódka mogła zapoznać się potencjalnie jedynie z P. po usługach bankowości elektronicznej (...). Przewodnik ten zawierał ogólne informacje o sposobie korzystania z bankowości internetowej. W części (...) wskazano by nigdy nie udostępniać hasła i numeru klienta osobom trzecim i nie podawać ich na nieszyfrowanych stronach (czyli takich, na których nie ma zainstalowanego certyfikatu bezpieczeństwa danej strony. Certyfikat można sprawdzić klikając w ikonę „kłódki"). Zalecono również upewnienie się czy system W. posiada najnowsze uaktualnienia oraz stosowanie najnowszych wersji przeglądarek internetowych oraz prowadzenie ich okresowej aktualizacji. Dopiero dnia 19 czerwca 2015 roku (a więc już po przedmiotowym zdarzeniu z dnia 25 i 25 maja 2015 roku) na stronie internetowej Banku pojawił się komunikat: „fałszywe komunikaty – nie otwieraj załączników". Można zakładać, że ta zwiększona akcja informacyjna była właśnie reakcją na masową akcję hakerską. Tym samym w sprawie nie udowodniono aby obecna, dużo większa świadomość na temat mechanizmów wyłudzeń danych autoryzacyjnych od klientów banków, była powszechna w maju 2015 roku. Z powyższego należy więc wnioskować, że ewentualne nabranie się przez powódkę na podstęp sprawców, stosujących nowe wówczas metody wyłudzeń, nie może być uznane za rażące niedbalstwo w przestrzeganiu zasady nieudostępniania narzędzi autoryzacyjnych

osobom postronnym. Na wysoką fachowość ataków phishingowych i ograniczoną możliwość uchronienia się przed nimi wskazywał także biegły A. N. (k. 428).

W konsekwencji Sąd nie stwierdził, by działaniu powódki można było przypisać cechy rażącego niedbalstwa. Pamiętać bowiem należy, iż rażące niedbalstwo jest kwalifikowaną formą winy nieumyślnej i sprowadza się do szczególnie wyraźnego braku staranności działania. Wobec tego, że pojęcie to ma charakter klauzuli generalnej, jego znaczenie zostało przybliżone przez orzecznictwo, w szczególności na kanwie art. 827 k.c. Jak wyjaśnił Sąd Najwyższy, "rażące niedbalstwo", to coś więcej niż brak zachowania zwykłej staranności w działaniu. Wykładnia tego pojęcia powinna zatem uwzględniać kwalifikowaną postać braku zwykłej lub podwyższonej staranności w przewidywaniu skutków działania. Chodzi tu o takie zachowanie, które graniczy z umyślnością (wyr. SN z 29.1.2009 r., V CSK 291/08, Biul. SN 2009, Nr 4, s. 16). Rażące niedbalstwo polega na przekroczeniu podstawowych, elementarnych zasad staranności (por. wyr SN z 16.1.2013 r., II CSK 202/12, L.). Ustalony stan faktyczny, do takich wniosków nie prowadził.

Mając na uwadze powyższe, w sprawie znalazł zastosowanie art. 46 ust. 1 u.u.p. skutkujący obowiązkiem Banku zwrotu kwoty nieautoryzowanej transakcji tj. kwoty 44 178 zł. Kwota ta podlegała jednakże pomniejszeniu o równowartość 150 euro zgodnie z dyspozycją art. 46 ust. 2 u.u.p. Jak już bowiem wcześniej wskazano, powódka nie zdołała udowodnić, by odpowiedzialność strony pozwanej mogła opierać się jedynie na nienależytym wykonaniu umowy o rachunek bankowy, co warunkowałoby wypłatę odszkodowania w pełnej wysokości. Przechodząc zaś na reżim odpowiedzialności z uwzględnieniem ustawy o usługach płatniczych, zastosowanie znaleźć musiał bezwzględnie wiążący art. 46 ust. 2 u.u.p. W sprawie za udowodnione należało bowiem uznać, niezależnie od braku szczegółowego wykazania przebiegu zdarzenia, że do nieautoryzowanej transakcji doszło wskutek posłużenia się utraconym lub skradzionym powódce instrumentem płatniczym. Ostatecznie z tego tytułu Sąd zasądził więc na rzecz powódki kwotę 43 558,82 zł (44 178 zł – 150 x 4,1279 zł).

Następnie, uznając że strona pozwana uchybiła obowiązkowi wynikającemu z art. 46 ust. 1 u.u.p. polegającemu na niezwłocznym przywróceniu obciążonego rachunku płatniczego do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza, na uwzględnienie zasługiwały także żądania powódki zasądzenia na jej rzecz kwoty 120 zł tytułem pobranych od niej 3 opłat za przelewy S. oraz kwoty 23,97 zł pobranych z rachunku tytułem 3 opłat za przelewy wewnętrzne między rachunkiem oszczędnościowym a oszczędnościowo – rozliczeniowym.

Łącznie z powyższych tytułów Sąd zasądził więc na rzecz powódki kwotę 43 702,79 zł.

Kolejno, Sąd zasądził na rzecz powódki także kwotę 15 zł jaką Bank pobrał z jej rachunku bankowego tytułem wysłania zawiadomienia o nieterminowej spłacie debetu – który w rzeczywistości, gdyby Bank wykonał w sposób prawidłowy zobowiązanie z art. 46 ust. 1 u.u.p. nie istniał. Podstawę odpowiedzialności Banku stanowił tu art. 471 k.c., w zw. z art. 725 k.c., tj. nienależyte wykonanie obowiązku prowadzenia rachunku bankowego poprzez wadliwe określenie jego salda i nieprawidłowe naliczenie z tego tytułu opłaty za wysłanie zaświadczenia.

Na analogicznej zasadzie Sąd uwzględnił także żądanie powódki zasądzenia na jej rzecz kwoty 465,86 zł pobranej z jej rachunku bankowego przez Bank tytułem odsetek od debetu, który w rzeczywistości nie istniał.

Łącznie zasądzono więc na rzecz powódki kwotę 44 183,65 zł (43 702,79 zł + 15 zł + 465,86 zł).

Odnośnie żądania odsetkowego, Sąd uwzględnił je jedynie w części. Od kwoty głównej 44 321,97 zł, powódka domagała się odsetek ustawowych za opóźnienie od dnia 27 maja 2019 roku, czyli dnia następnego po dniu dokonania przelewów z jej rachunku bankowego. W tym miejscu należy wskazać jednakże, że zgodnie z § 20 ust. 7 Regulaminu (...) Bank (...) S.A. rozpatruje reklamacje niezwłocznie, w terminie nie dłuższymi niż 30 dni. W przypadku braku możliwości rozpatrzenia reklamacji w tym terminie, (...) Bank (...) S.A. poinformuje klienta o planowanym terminie udzielenia odpowiedzi. Jak wynika z ustalonego stanu faktycznego powódka złożyła reklamację już dnia 26 maja 2015 roku. Termin na rozpatrzenie reklamacji upływał więc 25 czerwca 2015 roku. Pismem z dnia 17 czerwca 2015 roku Bank poinformował D. I., że jej reklamacja jest przedmiotem dalszej analizy, a czas jej rozpoznania może być wydłużony. Nie uzasadniono jednakże w żaden sposób przyczyny wydłużenia czasu rozpoznania reklamacji. Odpowiedź na reklamację

została wystosowana dopiero w kolejnym piśmie z dnia 31 lipca 2015. W ocenie Sądu, wobec nie wykazania przyczyn opóźnienia rozpoznania reklamacji w przewidzianym w Regulaminie terminie 30 dni, roszczenie stało się wymagalne z dniem 26 czerwca 2015 roku. Mając na uwadze powyższe, na podstawie art. 481 k.c., orzeczono jak w punkcie 1a) wyroku.

Odnośnie żądania zasądzenia odsetek od kwoty 15 zł oraz kwot składających się na sumę 465,86 zł wynikającą z pobranych przez Bank odsetek od debetu, Sąd także uwzględnił to żądanie jedynie w części. Zauważyć bowiem należy, iż żądanie zasądzenia kwot głównych opierało się na odszkodowaniu z tytułu nienależytego wykonania umowy rachunku bankowego, polegającego na niezasadnym pobraniu kwot z rachunku powódki. Spełnienie tego świadczenia przez Bank nie miało określonego terminu, więc stosownie do treści art. 455 k.c. stało się wymagalne niezwłocznie po wezwaniu do zapłaty. W aktach sprawy brak jest dowodów potwierdzających przedsądowe zwrócenie się przez powódkę do Banku o zwrócenie także i tych sum. Roszczenia te stały się więc wymagalne po upływie 30 dni na rozpoznanie reklamacji (§ 20 ust. 7 Regulaminu) tj. z dniem 4 kwietnia 2015 roku. Mając na uwadze powyższe, orzeczono jak w punkcie 1b) wyroku.

Oddaleniu (pkt 2 wyroku) podlegało więc jedynie żądanie główne w zakresie w jakim nie uwzględniało konieczności jego pomniejszenia o równowartość kwoty 150 euro oraz częściowo w zakresie odsetek, co szczegółowo omówiono powyżej.

O kosztach postępowania orzeczono w oparciu o zasadę odpowiedzialności za wynik sporu, obciążając nimi w całości stronę pozwaną. Sąd zastosował przy tym, dyspozycję art. 100 zd. 2 k.p.c., mając na uwadze, że powódka wygrała spór w przeszło 98%.

Na zasądzoną na rzecz powódki kwotę 5 372 zł składała się kwota 555 zł uiszczona przez powódkę tytułem części opłaty od pozwu oraz suma 4 800 zł tytułem wynagrodzenia ustanowionego przez powódkę w sprawie pełnomocnika będącego radcą prawnym, stosownie do dyspozycji § 2 pkt 5 rozporządzenia Ministra Sprawiedliwości w sprawie opłat za czynności radców prawnych z dnia 22 października 2015 r. (Dz.U. z 2015 r. poz. 1804 ze zm. w brzmieniu obowiązującym w dacie złożenia pozwu – 8 stycznia 2016 roku) powiększona o kwotę 17 zł tytułem opłaty skarbowej od pełnomocnictwa.

Jednocześnie w oparciu o treść art. 113 ust. 1 u.k.s.c., stosując tę samą zasadę odpowiedzialności za wynik sporu, Sąd nakazał pobrać od strony pozwanej na rzecz Skarbu Państwa – Sądu Rejonowego dla W. M.w W. kwotę 4 988,51 zł na którą składała się kwota 2 241 zł tytułem części nieuiszczonej przez powódkę opłaty od pozwu oraz wydatki poniesione tymczasowo z sum Skarby Państwa. W toku postępowania strona pozwana uiściła zaliczkę na poczet wynagrodzenia biegłego w kwocie 1 000 zł, z której wypłacono kwotę 785,31 zł biegłemu P. J. za sporządzenie opinii pisemnej. Reszta kwoty nie była dalej rozliczana, natomiast z S. Skarbu Państwa pokryto następujące wydatki: 293,26 zł tytułem zwrotu kosztów podróży świadka, 1 122,49 zł (opinia główna biegłego A. N.), 505,09 zł (pisemna opinia uzupełniająca biegłego A. N.), 1 041,36 zł (ustna opinia uzupełniająca biegłego A. N.). Łącznie wydatki pokryte z sum Skarbu Państwa i z zaliczki wyniosły więc 5 988,51 zł. Pomniejszając je o kwotę 1 000 zł, stanowiącą wartość uiszczonej przez stronę pozwaną zaliczki, do pokrycia pozostawała wartość 4 981,55 zł, którą nakazano pobrać od strony pozwanej w pkt. 4 wyroku.

Mając na uwadze powyższe, orzeczono jak w sentencji.

Z/ (...).