Sygnatura akt VIII C 873/18

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 17 lutego 2021 roku

Sąd Rejonowy dla Łodzi - Widzewa w Łodzi VIII Wydział Cywilny w składzie:

Przewodniczący: Sędzia Małgorzata Sosińska-Halbina

Protokolant: st. sekr. sąd. Izabella Bors

po rozpoznaniu w dniu 17 lutego 2021 roku w Łodzi

na rozprawie

sprawy z powództwa M. K.

przeciwko (...) Bank (...) Spółce Akcyjnej z siedzibą w W.

o zapłatę

1. zasądza od pozwanego na rzecz powódki kwotę 19.963 zł (dziewiętnaście tysięcy dziewięćset sześćdziesiąt trzy złote) z ustawowymi odsetkami za opóźnienie od dnia 6 czerwca 2017 roku do dnia zapłaty;

2. zasądza od pozwanego na rzecz powódki kwotę 3.917 zł (trzy tysiące dziewięćset siedemnaście złotych) tytułem zwrotu kosztów procesu;

3. nakazuje pobrać od pozwanego na rzecz Skarbu Państwa Sądu Rejonowego dla Łodzi-Widzewa w Łodzi kwotę 234,71 zł (dwieście trzydzieści cztery złote siedemdziesiąt jeden groszy) tytułem nieuiszczonych kosztów sądowych.

Sygn. akt VIII C 873/18

UZASADNIENIE

W dniu 17 kwietnia 2018 roku powódka M. K., reprezentowana przez zawodowego pełnomocnika, wytoczyła przeciwko Bankowi (...) Spółce Akcyjnej z siedzibą we W. (obecnie (...) Bank (...) S.A. w W.) powództwo o zapłatę kwoty 19.963 zł wraz z ustawowymi odsetkami za opóźnienie od dnia 6 czerwca 2017 roku do dnia zapłaty oraz wniosła o zasądzenie zwrotu kosztów procesu według norm przepisanych.

W uzasadnieniu pozwu pełnomocnik powódki wskazał, że w dniu 19 lutego 2014 roku ta zawarła z pozwanym umowę o prowadzenie rachunku bankowego, na mocy której otwarto dla klientki rachunek internetowy.

W dniach 16 i 17 kwietnia 2017 roku nieznany sprawcy wykonał bez wiedzy i zgody powódki cztery operacje bankowe przelewając z jej rachunku o numerze (...) (...) 3410 na zewnętrzny rachunek bankowy o numerze 10 2490 (...) (...) łączną kwotę 19.963 zł. Powódka nie składała polecenia wykonania wskazanych transakcji, nie wyrażała na nie zgody i nie wiedziała o nich. O powyższych transakcjach powódka powzięła wiedzę w dniu 5 maja 2017 roku i wówczas niezwłocznie poinformowała o zdarzeniu pozwanego oraz wypowiedziała umowę usług bankowości elektronicznej ze skutkiem natychmiastowym z uwagi na uzasadnione podejrzenie popełnienia przestępstwa. Tego samego dnia ojciec powódki zgłosił zdarzenie na policji. W dniu 24 maja 2017 roku pozwany, w odpowiedzi na reklamację powódki, poinformował ją, że przedmiotowe przelewy zostały prawidłowo zrealizowane, zgodnie ze złożonymi dyspozycjami. Wskazał, że nie można wykluczyć działania złośliwego oprogramowania na urządzeniu, które było narzędziem do złożenia tych transakcji lub przejęcia kontroli na routerem, i że w ten sposób mogło nastąpić przekierowanie na

fałszywą stronę usług bankowości elektronicznej. Jednocześnie podniósł, iż nie wystąpiły nieprawidłowości w pracy systemów bankowych, jak również naruszenia, czy też próby naruszenia zabezpieczeń po stronie banku. Pismem z dnia 18 lipca 2017 roku powódka wezwała pozwanego do dobrowolnej zapłaty na jej rzecz kwoty 19.963 zł, ale ten ponownie odmówił zwrotu środków. W dalszej kolejności pełnomocnik powódki podniósł, że ryzyko dokonania wypłaty z rachunku bankowego, w tym rachunku internetowego, do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża bank. Wynika to z ustawy o usługach płatniczych, która przewiduje generalną zasadę, że dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika. Ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika spoczywa przy tym na dostawcy tego użytkownika. Jednocześnie powódka nie naruszyła obowiązków, o których mowa w art. 42 ustawy, umyślnie lub wskutek rażącego niedbalstwa.

(pozew k. 51-56)

W odpowiedzi na pozew strona pozwana, reprezentowana przez zawodowego pełnomocnika, wniosła o oddalenie powództwa w całości oraz o zasądzenie zwrotu kosztów procesu według norm przepisanych.

W uzasadnieniu strona pozwana wyjaśniła, że sporne transakcje zostały wykonane z rachunku powódki zgodnie z umową usług bankowości elektronicznej oraz zgodnie z zasadami korzystania z usług bankowości elektronicznej. Autoryzacje dyspozycji odbyły się po poprawnym zalogowaniu do usług bankowych, tj. po podaniu numeru identyfikacyjnego NIK oraz po poprawnym wprowadzeniu hasła, przy użyciu narzędzia autoryzacyjnego przypisanego do powódki, tj. smsKodu wysłanego na numer (...). W ten sposób w dniu 16 kwietnia 2017 roku został dodany nowy odbiorca do rachunków zaufanych. Jednocześnie nie nastąpiło naruszenie zabezpieczeń Banku, czy włamanie do sytemu bankowego. Zdarzenie nie było też efektem awarii, czy zaniedbania po stronie pozwanego. Niezależnie od powyższego pozwany wyjaśnił, że nawet gdyby sporne dyspozycje nie były objęte wolą powódki i do ich złożenia doszło w wyniku przestępstwa, to powódce można przypisać rażące niedbalstwo. Powódka poprzez wpisanie przesłanego jej sms-em kodu dodała zaufanego odbiorcę, choć dane odbiorcy przesłane w wiadomości winny wzbudzić jej podejrzenie. Powódka przy korzystaniu z bankowości elektronicznej winna przy tym sprawdzić certyfikat serwera, zwłaszcza, że co najmniej dwukrotnie była informowana przez bank o istnieniu zagrożenia ataku hakerskiego. Pozwany zaznaczył ponadto, że obowiązkiem użytkownika jest posiadanie odpowiednich zabezpieczeń narzędzi do logowania, a także niezwłoczne poinformowanie banku o kradzieży. Jak wynika zaś z danych logowania, powódka po wykonaniu spornych przelewów w dniu 18 kwietnia 2017 roku zalogowała się do bankowości elektronicznej, jednakże zgłoszenia kradzieży dokonała dopiero w dniu 5 maja 2017 roku.

W przypadku nie podzielenia powyższej argumentacji, z ostrożności procesowej, pozwany wniósł o ograniczenie jego odpowiedzialności o kwotę 150 euro z uwagi na treść art. 46 ust. 2 w zw. z art. 42 ust. 2 ustawy o usługach płatniczych.

(odpowiedź na pozew k. 81-85)

W toku procesu stanowiska stron nie uległy zmianie. Pełnomocnik powódki dodatkowo podniósł, że udzielenie zgody przez płatnika jest jedyną przesłanką autoryzacji danej transakcji płatniczej. Dopiero w takim przypadku można mówić o prawidłowym jej wykonaniu. Jeżeli zgoda na transakcję płatniczą została udzielona przez podmiot do tego nieuprawniony, a dostawca wykonuje taką transakcję, to nie zyskuje on uprawnienia ani do obciążenia rachunku płatnika, ani do żądania od płatnika zwrotu kwoty, którą przekazał dostawcy usług płatniczych odbiorcy. Pełnomocnik pozwanego uzupełniająco wyjaśnił z kolei, że podczas logowania w dniu 18 kwietnia 2017 roku sprawdzana była historia dyspozycji i historia rachunku,
zaś w dniu 5 maja 2017 roku historia rachunku.

(protokół rozprawy k. 136-143, k. 169-174, k. 181-183, k. 253-255, k. 268-270, k. 287-288, pismo procesowe k. 147-148v., k. 213-214, k. 216-219, k. 237-239, k. 262-263v., k. 271-275)

Sąd Rejonowy ustalił następujący stan faktyczny:

W dniu 19 lutego 2014 roku powódka M. K., zawarła z poprzednikiem prawnym pozwanego - Bankiem (...) S.A. umowę rachunku oszczędnościowo-rozliczeniowego, umowę usług bankowości elektronicznej (...), umowę o kartę płatniczą oraz umowę o elektroniczny instrument płatniczy. Na mocy rzeczonej umowy bank otworzył oraz zobowiązał się prowadzić dla posiadacza rachunek oszczędnościowo-rozliczeniowy, a także udostępnić posiadaczowi dostęp do usług bankowości elektronicznej (...). W ramach tych ostatnich powódce przypisano numer NIK – (...) oraz ustalono limitu przelewów na kwotę 100 zł dziennie (limit z autoryzacją smsKodem) i 50 zł (limit bez autoryzacji smsKodem). Autoryzacja była przesyłana na podany przez powódkę numer telefonu
– (...). Umowa została zawarta na czas nieoznaczony z zastrzeżeniem, że zawarcie nowej umowy usług bankowości elektronicznej (...) powoduje utratę mocy obowiązującej niniejszej umowy z tym zastrzeżeniem, że pozostają w mocy dotychczas wykorzystywane przez posiadacza hasła (...) niezbędne do korzystania z usług (...).

W dniu zawarcia umowy powódka była małoletnia – nie miała ukończonych 15 lat (ur. (...)).

W dniu 17 sierpnia 2015 roku strony zawarły umowę usług bankowości elektronicznej (...), która zastąpiła pierwotną umowę w tym zakresie. Umowa ta odpowiadała treści uprzedniej, z tą różnicą, że limit przelewów bez autoryzacji smsKodem został określony na kwotę 10.000 zł. Jako telefon do smsKodu wskazano (...).

Aneksem z dnia 10 stycznia 2017 roku M. K. zmieniła numer telefonu przypisany do metody autoryzacji na (...).

(umowa k. 63-65, umowa k. 176-177, aneks k. 111, okoliczności bezsporne)

Zgodnie z Z. korzystania z usług bankowości elektronicznej (...) dla ludności, NIK to nadawany przez bank numer identyfikacyjny klienta składający się z 8 cyfr, który jest wykorzystywany przez klienta w celu identyfikacji przy uruchamianiu i korzystaniu z usług (...). Z kolei (...) to hasło identyfikujące klienta zapewniające klientowi wyłączność dostępu do usług (...), znane wyłącznie klientowi, któremu zostało wydane. Oświadczenie woli klienta złożone za pośrednictwem usług (...) i autoryzowane w sposób właściwy dla danego oświadczenia, w tym zlecenie płatnicze w rozumieniu (...), nosiło nazwę dyspozycji. Autoryzacja oznaczała udzielenie przez klienta zgody na wykonanie dyspozycji przed jej realizacją przez bank, w sposób określony w umowie lub niniejszych zasadach. SmsKod zdefiniowany został, jako jednorazowy kod przesyłany na żądanie klienta na jego numer telefonu komórkowego wskazany w umowie, służący do identyfikacji klienta i autoryzacji dyspozycji klienta w ramach usług (...).

W myśl § 13, identyfikacja klienta w usłudze (...) polegała co do zasady na prawidłowym podaniu numer NIK i hasła (...). Opcjonalnie, na życzenie klienta, identyfikacja mogła obejmować dodatkowo podanie smsKodu przesłanego na telefon komórkowy klienta. Sposób autoryzacji dyspozycji w usługach (...) internet następował poprzez wybranie na ekranie odpowiedniego przycisku i – w przypadku, gdy dla danej dyspozycji wymagane jest potwierdzenie smsKodem – podanie również smsKodu przesłanego na telefon komórkowy. Klient mógł przy tym poprzez złożenie odpowiedniej dyspozycji w usłudze (...) internet uczynić wybranych odbiorców zaufanymi odbiorcami przelewów. Dyspozycje przelewów na rachunku prowadzone na rzecz zaufanych odbiorców mogły być składane w usłudze (...),
a ich autoryzacja następowała wyłącznie poprzez wybranie na ekranie odpowiedniego przycisku (§ 16 ust. 7 i 8). Bank przystępował do realizacji dyspozycji w usługach (...) z chwilą jej otrzymania, jednak nie później niż do końca następnego dnia roboczego banku. Momentem otrzymania dyspozycji przez bank było dokonanie autoryzacji dyspozycji przez klienta (§ 19 ust. 1 i 3). Klient zobowiązany był stosować się do zaleceń banku w zakresie zasad bezpieczeństwa usług (...), w szczególności winien z należytą starannością chronić numer NIK, hasła (...), dodatkowe hasło/hasło dostępu, smsKody, telefon komórkowy, jeżeli jego numer jest udostępniony bankowi w celu identyfikacji klienta lub autoryzacji jego dyspozycji. Klient ponosił pełną odpowiedzialność za ich udostępnienie osobom trzecim (§ 38 ust. 1). W trakcie korzystania z usługi (...) internet komunikacja pomiędzy komputerem klienta a serwerem banku była szyfrowana protokołem (...) z zastosowaniem certyfikatu wystawionego i uwierzytelnionego dla serwera bankowego o nazwie centrum24.pl lub bzwbk24.pl. (...) zalogowaniem się klient, aby upewnić się, że rzeczywiście nawiązał połączenie z serwerem banku, powinien sprawdzić certyfikat serwera (§ 38 ust. 5). Klient nie powinien używać do logowania do usługi (...) internet adresu lub linku przesłanego drogą elektroniczną albo za pomocą komunikatorów internetowych i innych narzędzi służących do komunikowania się w internecie (§ 38 ust. 6).

Klient zobowiązany był do należytego zabezpieczenia urządzeń z wykorzystaniem których uzyskuje dostęp do usług (...) oraz zobowiązany do ich ochrony przed złośliwym oprogramowaniem lub dostępem osób nieuprawnionych poprzez: zainstalowanie na urządzeniu legalnego oprogramowania systemowego oraz antywirusowego, stosowanie zapory sieciowej, dokonywanie aktualizacji zainstalowanego na urządzeniu oprogramowania, nie instalowanie oprogramowania nieznanego pochodzenia, nie otwieranie i nie odpowiadanie na wiadomości email od nieznanych nadawców, nie otwieranie plików niewiadomego pochodzenia (§ 38 ust. 9). Klient powinien poinformować niezwłocznie bank o wszelkich podejrzanych przypadkach związanych z korzystaniem z usług (...), w szczególności o próbie dostępu do usług (...) lub korzystania z usług (...) przez osoby nieuprawnione (§ 38 ust. 13). Szczegółowe informacje dotyczące zasad bezpieczeństwa usług (...) zamieszczane były na portalu banku (§ 38 ust. 16).

(Zasady korzystania z usług bankowości elektronicznej (...) k. 98-108)

SmsKody są generowane przez algorytmy szyfrujące w ten sposób, że z systemu przychodzi informacja o operacji, którą klient zamierza wykonać, i specjalnie dla tej operacji jest generowany kod. Po wpisaniu kodu przez klienta system weryfikuje jego poprawność i autoryzuje transakcję. Wygenerowany kod ważny jest przez 2 minuty. W treści smsKodu zamieszczana jest krótka informacja o planowanej transakcji,
m.in. wpisana jest kwota przelewu i numer rachunku odbiorcy. W przypadku odbiorców zaufanych smsKod nie jest wymagany, a lista takich odbiorców jest przypisana do NIK-u klienta. Pracownicy banku nie mają dostępu do haseł klientów.

Jest możliwe podpięcie się pod system operatora telefonicznego i przechwycenie wiadomości SMS.

To samo urządzenie może mieć różne numery IP.

(zeznania świadka M. P. 00:07:49-00:49:33 elektronicznego protokołu rozprawy z dnia 28 listopada 2018 roku – k. 137-139)

W czerwcu i lipcu 2016 roku pozwany bank przesłał na pocztę email powódki ostrzeżenia przed oszustwami internetowymi polegającymi na wyłudzeniu danych do logowania.

W 2017 roku powódka dostawała dużo smsów z banku z ofertami różnych produktów bankowych, nie zawsze odczytywała te wiadomości.

(wydruk wiadomości email k. 94-94v., dowód z przesłuchania powódki 00:07:57-00:26:34 elektronicznego protokołu rozprawy z dnia 25 września 2019 roku – k. 182-183)

Nieustalona osoba trzecia, wbrew woli i bez wiedzy powódki, pozyskała login (NIK) i hasło ((...)) do jej rachunku bankowego.

W dniu 16 kwietnia 2017 roku, tj. w Niedzielę Wielkanocną, w godzinach wieczornych, osoba trzecia zalogowała się na konto powódki, gdzie złożyła dyspozycję utworzenia zaufanego odbiorcy. Powódka nie miała świadomości powyższego i nie zamierzała wprowadzić żadnego zaufanego odbiorcy. O godzinie 22:11:36 na telefon komórkowy o numerze (...), służący do autoryzacji dyspozycji, został wysłany smsKod o treści „dodanie odbiorcy 10 2490 (...) (...)", dla której to dyspozycji został wygenerowany kod o numerze (...). O godzinie 22:12:46 przedmiotowy kod został wprowadzony do systemu bankowego z IP 80.48.60.206 (Telefony (...)). O godzinie 22:12:46 utworzono odbiorcę o nazwie „vcbxcvbxvcbvxcbxc" z numerem konta 10 2490 (...) (...). Autoryzacja nastąpiła z numeru IP 80.48.60.206 (Telefony (...)). O godzinie 22:41:16 z adresu IP 91.195.57.183 ((...)K.) złożono dyspozycję przelewu (bez autoryzacji) na konto zaufanego odbiorcy na kwotę 4.989 zł. O godzinie 22:42:00 z tego samego numeru IP złożono dyspozycję przelewu (bez autoryzacji) na konto zaufanego odbiorcy na kwotę 4.993 zł. Dnia 17 kwietnia 2017 roku, o godzinie 00:13:19 z adresu IP 83.1.196.201 (Telefony (...)) złożono dyspozycję przelewu (bez autoryzacji) na konto zaufanego odbiorcy na kwotę 4.999 zł. Wreszcie, o godzinie 00:13:43 z tego samego numeru IP (83.1.196.201) złożono dyspozycję przelewu (bez autoryzacji) na konto zaufanego odbiorcy na kwotę 4.982 zł.

Jak wskazał powołany w sprawie biegły, przedmiotowy atak najprawdopodobniej był prowadzony z dwóch miejsc i przebiegał w czterech fazach:

1) pozyskanie danych do logowania na konto powódki przez nieznane osoby,

2) utworzenie zaufanego odbiorcy z adresu IP w sieci (...) SA oraz przechwycenie treści wiadomości SMS i dokonanie autoryzacji z tego samego IP,

3) dokonanie dwóch przelewów z IP z sieci (...)K.,

4) dokonanie dwóch przelewów z sieci (...) SA.

Formalnie nie nastąpiło naruszenie zasad bezpieczeństwa teleinformatycznego, regulaminu bankowego ani procesu autoryzacji transakcji: nastąpiło logowanie za pomocą znanego konta użytkownika, podano poprawne hasło i numer z smsKodu. Bank wprowadził stosowne zabezpieczenia według normy (...):2013. Zabezpieczenia te nie były jednak wystarczające i zostały przełamane przez twórców procesu kradzieży. Sprawcy wykorzystali słabości uwierzytelniania transakcji za pomocą SMS.

Do przeprowadzenia przedmiotowego ataku nie było konieczne wykorzystanie złośliwego oprogramowania (wirusa), a jedynie podrobienie witryny banku. Do fałszywej bankowości elektronicznej można wejść przypadkowo, m.in. z serwisów zakupowych.

Po dokonaniu kradzieży środków saldo na rachunku bankowym powódki wynosiło 6.664,45 zł.

(pisemna opinia biegłego sądowego k. 199-206v., pisemna uzupełniająca opinia biegłego sądowego k. 227-230, historia operacji k. 67, dane logowania k. 91-93, dowód z przesłuchania powódki 00:07:57-00:26:34 elektronicznego protokołu rozprawy z dnia 25 września 2019 roku
– 182-183)

W dniu 18 kwietnia 2017 roku o godzinie 19:57:37 nastąpiło logowanie na konto bankowe powódki z adresu IP 94.254.131.236, a następnie osoba logująca się sprawdziła historię rachunku. Jeszcze tego samego dnia, o godzinie 20:04:23 miało miejsce drugie logowanie do konta, tym razem z adresu IP 188.146.134.142.

(dane logowania k. 91-93)

W dniu 5 maja 2017 roku powódka zamierzała kupić przez Internet bilet na przejazd autobusem na trasie Ł.-K., za który chciała zapłacić dokonując przelewu ze swojego konta. Strona przewoźnika, z którego usług powódka zamierzała wówczas pierwszy raz skorzystać była inna niż te, z których dotychczas korzystała i wymagała innej procedury zapłaty ceny – koniecznym było zalogowanie na konto i dokonanie płatności. Po zalogowaniu się na konto M. K. wraz z matką spostrzegły, że zostały na nim wykonane 4 nieznane im przelewy na sporną kwotę. Jeszcze tego samego dnia powódka wraz z ojcem pojechała do pozwanego banku, gdzie złożyła reklamację. Dopiero w banku powódka odnotowała, że na jej telefon przyszedł w kwietniu sms informujący o dodaniu nowego podmiotu do grupy zaufanych odbiorców. W tym czasie do powódki przychodziło jednak dużo smsów z pozwanego Banku z ofertami handlowymi, których powódka, nie będąc nimi zainteresowaną, nie czytała. W sporządzonym tego dnia aneksie do umowy usług bankowości elektronicznej (...) odręczny zapis „usługi elektroniczne zostały zamknięte w celu zachowania bezpieczeństwa do kont klienta". M. K. złożyła wówczas pozwanemu również oświadczenie o wypowiedzeniu z dniem 5 maja 2017 roku umowy usług bankowości elektronicznej (...).

Po wizycie w banku powódka wraz z ojcem dokonała zgłoszenia zdarzenia na Policji składając zawiadomienie o podejrzeniu popełnienia przestępstwa.

Pismem z dnia 24 maja 2017 roku pozwany odmówił uwzględnienia reklamacji podnosząc, że przelewy zostały zrealizowane poprawnie, zgodnie ze złożonymi dyspozycjami.

(dowód z przesłuchania powódki 00:07:57-00:26:34 elektronicznego protokołu rozprawy z dnia 25 września 2019 roku – k. 182-183, 00:04:03-00:28:00 elektronicznego protokołu rozprawy z dnia 29 lipca 2020 roku – k. 214-215, zeznania świadka K. R. 00:18:00-00:29:37 elektronicznego protokołu rozprawy z dnia 15 maja 2019 roku – k. 171, zeznania świadka P. K. 00:31:00-00:44:15 elektronicznego protokołu rozprawy z dnia 15 maja 2019 roku – k. 172-173, aneks k. 66, wypowiedzenie k. 68, pismo z dn. 24.05.2017r. k. 73-74)

Pismem z dnia 18 lipca 2017 roku powódka ponownie wezwała pozwanego do zapłaty w terminie 7 dni kwoty 19.963 zł tytułem zwrotu nieautoryzowanej transakcji płatniczej. W odpowiedzi pozwany wyjaśnił, że sporne przelewy zostały zrealizowane poprawnie, zgodnie ze złożonymi dyspozycjami. Pozwany wskazał,
że w zaistniałej sytuacji nie można wykluczyć działania złośliwego oprogramowania na urządzeniu, które było narzędziem do złożenia transakcji lub przejęcia kontroli nad routerem, a także, że osoba dokonująca przelewów wykorzystała funkcjonalność polegającą na dopisaniu odbiorcy jako tzw. rachunek zaufany na liście odbiorców. Czynność ta wymagała jednak autoryzacji, która została przeprowadzona przez powódkę. Pozwany podniósł ponadto, że nie wystąpiły nieprawidłowości w pracy systemów bankowych, jak również naruszenia, czy też próby naruszenia zabezpieczeń po stronie banku.

(wezwanie do zapłaty k. 70-72, pismo k. 73-74, k. 75-76)

Środki zgromadzone na rachunku powódki, wpłacane przez jej rodziców i dziadków, miały stanowić prezent dla M. K. na jej osiemnaste urodziny, które miały miejsce niecałe pół roku po zdarzeniu. Konto to było bardzo rzadko używane - powódka sporadycznie korzystała wówczas z dostępnych środków dokonując jedynie drobnych zakupów przez Internet i płacąc najczęściej za pośrednictwem strony internetowej sklepu. Powódka zawsze używała w tym celu swojego laptopa.

Powódka nie udostępniała nikomu żadnych danych do logowania w bankowości elektronicznej, czy innych danych koniecznych do przeprowadzania jakichkolwiek transakcji związanych z bankowością elektroniczną. Laptop powódki, z którego korzystała, miał zabezpieczenie antywirusowe.

(dowód z przesłuchania powódki 25 września 2019 roku - k. 182-183 i 00:04:03-00:28:00 elektronicznego protokołu rozprawy z dnia 29 lipca 2020 roku – k. 214-251, zeznania świadka K. R. 00:18:00-00:29:37 elektronicznego protokołu rozprawy z dnia 15 maja 2019 roku – k. 171, zeznania świadka P. K. 00:31:00-00:44:15 elektronicznego protokołu rozprawy z dnia 15 maja 2019 roku – 172-173)

W sprawie przedmiotowego zdarzenia było prowadzone przez prokuraturę postępowanie przygotowawcze, w toku którego nie udało się ustalić sprawców przestępstwa ani odnaleźć skradzionych środków. W ramach postępowania oględzinom został poddany laptop powódki, na którym nie znaleziono żadnych nieprawidłowości.

Jesienią 2017 roku powódka była przesłuchiwana jako świadek w innej sprawie karnej, dotyczącej analogicznej kradzieży, która miała miejsce na Śląsku. W obu przypadkach skradzione środki zostały przelane na to samo konto, na które przelano środki z rachunku powódki.

W dniu 18 kwietnia 2017 roku również inny posiadacz rachunku w pozwanym banku (...) odnotował brak środków na koncie, których dyspozycji przelewu nie zlecał. Nieznana osoba dokonała wówczas czterech przelewów potwierdzanych smsKodem, których on nie zlecał i nie potwierdzał smsKodem. Sprawa karna, wszczęta z jego zawiadomienia o podejrzeniu popełnienia przestępstwa została umorzona wobec niewykrycia sprawców. Od prowadzących sprawę policjantów świadek otrzymał wówczas informację o analogicznych, innych sytuacjach z udziałem pozwanego banku.

(dowód z przesłuchania powódki 00:07:57-00:26:34 elektronicznego protokołu rozprawy z dnia 25 września 2019 roku - k. 182-183, zeznania świadka K. R. 00:18:00-00:29:37 elektronicznego protokołu rozprawy z dnia 15 maja 2019 roku - k. 171, zeznania świadka P. K. 00:31:00-00:44:15 elektronicznego protokołu rozprawy z dnia 15 maja 2019 roku

– 172-173, zeznania świadka D. C. 00:07:12 – 00:14:48 elektronicznego protokołu rozprawy z dnia 15 października 2020 roku – 269-270)

Jest cały szereg przestępstw w bankowości elektronicznej. Przykładowo na samych kartach przestępstwo może być dokonane za pomocą ok. 100 różnych, metod.

Zdaniem biegłego najbardziej prawdopodobnym w przedmiotowej sprawie jest, że atak był przeprowadzony metodą phisingu.

(zeznania świadka P. L. 00:50:00-01:22:00 elektronicznego protokołu rozprawy z dnia 28 listopada 2018 roku – k. 142, pisemna opinia biegłego sądowego k. 199-206v.)

Czytanie ze zrozumieniem certyfikatu bezpieczeństwa wymaga wiedzy specjalistycznej.

Instalacja na komputerze klienta oprogramowania antywirusowego jest niewystarczająca do uniemożliwienia przeprowadzenia ataku pishingowego. Użytkownik komputera nie ma możliwości posiadania oprogramowania antywirusowego zawierającego aktualną bazę wirusów. Przedmiotowe oprogramowanie nie zadziała poprawnie, gdy pojawi się nieznane złośliwe oprogramowanie, przykładowo napisane do ataku dedykowanego na ustalonego użytkownika.

Bank powinien przyjąć, że każdy komunikat pochodzący od użytkownika może być obciążony złośliwą treścią. Każdy komunikat przychodzący do banku z zewnątrz musi być traktowany ze szczególną ostrożnością – m.in. w celu oddzielenia potencjalnie złośliwych treści od właściwego komunikatu. Dowolny ciąg znaków przychodzący do banku z zewnątrz musi być traktowana jako potencjalnie niebezpieczny.

Adres IP jest to unikalny w skali świata adres związany z urządzeniem mającym bezpośredni dostęp do Internetu (serwer, router, urządzenie brzegowe).

Numer IP składa się z czterech liczb z przedziału od 0 do 255. Adres IP 94.254.130.178 należy do przedziału 94.254.128.0-94.254.191.255 z puli (...) (P. P. Sp. z o.o.). Adres IP 188.146.69.176 należy do przedziału 188.146.0.0-188.147.127.255 z puli E. (blueconnect (...) S.A.). W okresie od dnia 3 marca 2014 roku do dnia 5 maja 2017 roku użytkownik (...) logował się do usług pozwanego z adresów wchodzących w skład rzeczonych puli (do puli (...) w dniach 16 kwietnia 2017 roku (x2), 18 kwietnia 2017 roku (x2), 5 maja 2017 roku (x2); do puli E. w dniach 1 czerwca 2016 roku (x3), 4 listopada 2016 roku (x2), 10 stycznia 2017 roku, 18 kwietnia 2017 roku, 5 maja 2017 roku (x2).

Określenie lokalizacji na podstawie adresu IP jest możliwe, jednak nie w sposób precyzyjny, ponieważ dla adresów z puli podawany jest najczęściej adres właściciela, a nie klienta znajdującego się być może w odległej lokalizacji, co ma miejsce szczególnie często dla adresów z puli dostawców telefonii. Większe firmy, dostawcy usług (...), firmy telefonii komórkowej i inne rezerwują dla swoich klientów pewne zakresy adresów IP, przydzielając je następnie dynamicznie (według potrzeb) lub statycznie swoim klientom.

Adres IP 188.146.134.142 (T-M.) jest adresem mobilnym, przyznawanym losowo w jednym czasie do połączeń z Internetem wielu różnym użytkownikom.

W sieci P. wiele urządzeń może posiadać ten sam adres IP, a różnić się używanymi portami. Obecnie jeden adres IP może być przydzielony ***jednocześnie do około 2 tysięcy urządzeń***. Bez wskazania portu źródłowego połączenia w Internecie nie jest możliwe rozstrzygnięcie, które z tych urządzeń łączyło się w podanym czasie z określoną stroną internetową. W sieci P. adresy IP przydzielane są dynamicznie, tj. tylko na czas jednej sesji internetowej (lub jej części). Po zakończeniu sesji zwolnione adresy IP są przydzielane kolejnym terminalom.

Dostawcy Internetu automatycznie niszczą dane wykraczające poza okres 12 miesięcy licząc od dnia połączenia lub nieudanej próby połączenia.

To samo urządzenie może mieć różne IP.

Nie jest jasne, w jaki sposób osoba trzecia uzyskała smsKod przesłany z banku na numer telefonu powódki.

(pisemna opinia biegłego sądowego k. 199-206v., pisemna uzupełniająca opinia biegłego sądowego k. 227-230, pismo T-M. k. 295, pismo P. k. 293)

Powyższy stan faktyczny Sąd ustalił bądź jako bezsporny, bądź na podstawie znajdujących się w aktach sprawy dowodów z dokumentów, które nie budziły wątpliwości, co do prawidłowości ani rzetelności ich sporządzenia, nie były także kwestionowane przez żadną ze stron procesu. Za podstawę ustaleń faktycznych Sąd przyjął również zeznania powódki, powołanych w sprawie świadków oraz opinię biegłego sądowego. Oceniając opinię biegłego, Sąd nie znalazł podstaw do kwestionowania zawartych w jej treści wniosków, opinia ta była bowiem rzetelna, jasna, logiczna oraz w sposób wyczerpujący objaśniająca budzące wątpliwości kwestie. Wydając opinię biegły oparł się na zgromadzonym w aktach sprawy materiale dowodowym. Opinia biegłego stanowi przekonujący i miarodajny dowód w sprawie. Opinia ta odzwierciedla staranność i wnikliwość w badaniu zleconego zagadnienia, wyjaśnia wszystkie istotne okoliczności, podaje przyczyny, które doprowadziły do przyjętej konkluzji, a równocześnie jest poparta głęboką wiedzą i wieloletnim doświadczeniem zawodowym biegłego, który był m.in. biegłym z zakresu informatyki w Międzynarodowym Trybunale Karnym w H.. Jednocześnie, w ocenie Sądu, opinii tej nie podważają pozostałe dowody zebrane w sprawie, nie była ona ostatecznie kwestionowana przez strony procesu, ma ona także kategoryczny charakter. W konsekwencji Sąd uznał, że opinia biegłego sądowego stanowi pełnowartościowy dowód, który może być podstawą czynionych w sprawie ustaleń faktycznych.

Sąd Rejonowy zważył, co następuje:

Powództwo jest usprawiedliwione w całości.

Rozważania w sprawie rozpocząć należy od przypomnienia treści art. 725 k.c., w myśl której, 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. Zgodnie z 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.

W konsekwencji pomimo 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 (por. postanowienie SN z dnia 28 kwietnia 2016 roku, I KZP 3/16, L.).

Ze swojego długu wobec posiadacza rachunku bank nie zwolni się nawet wtedy, gdy dochowa należytej staranności przy dokonywaniu wypłaty osobie nieuprawnionej. Ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową. Równoległą podstawą odpowiedzialności banku jest bowiem także ustawa z 19 sierpnia 2011 roku o usługach płatniczych, zwana dalej „ustawą". Przywołana ustawa określa między innymi prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych, a także zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych (art. 1 pkt 2 ustawy). Bank krajowy jest dostawcą usług płatniczych w rozumieniu ustawy
(art. 4 ust. 1 i ust. 2 pkt 1).

Przez usługi płatnicze rozumie się działalność polegającą w szczególności na wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy przez wykonywanie usług polecenia przelewu (art. 3 pkt 2 lit. c).

Płatnikiem w rozumieniu ustawy jest m. in. osoba fizyczna, składająca zlecenie płatnicze, czyli oświadczenie skierowane do dostawcy zawierające polecenie wykonania transakcji płatniczej (art. 2 pkt 22 i pkt 36). Zlecenie płatnicze, zgodnie
z art. 2 pkt 10 ustawy, płatnik składa przy użyciu instrumentu płatniczego, którym jest zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego.

W przedmiotowej sprawie zgoda na wykonanie transakcji płatniczych za pośrednictwem usług bankowości elektronicznej świadczonych przez pozwany Bank miała być udzielana przez powódkę po zalogowaniu się do konta za pomocą danych identyfikacyjnych, tj. numeru NIK i hasła oraz po podaniu smsKodu przesłanego na telefon komórkowy powódki.

Na pozwanym Banku jako dostawcy wydającemu instrument płatniczy ciążył z mocy art. 43 pkt 1 ustawy obowiązek zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, na powódce zaś - jako użytkowniku instrumentu płatniczego – spoczywał obowiązek korzystania z instrumentu płatniczego zgodnie z umową bankową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu (art. 42 ust. 1 pkt 1 i 2). W celu spełnienia powyższego obowiązku użytkownik, z chwilą otrzymania instrumentu płatniczego, winien podejmować niezbędne środki zapobiegające naruszeniu indywidualnych zabezpieczeń instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (art. 42 ust. 2).

Pozwany bank, jako profesjonalny podmiot nie wywiązał się ze swoich obowiązków względem powódki. Jak wynika z opinii powołanego w sprawie biegłego Bank wprowadził wprawdzie stosowne zabezpieczenia wymagane normą (...):2013 ale niewątpliwie sam fakt kradzieży środków z rachunku powódki oznacza, że zabezpieczenia te nie były wystarczające i zostały przełamane przez twórców złośliwego oprogramowania i procesu kradzieży. Gdyby zabezpieczenia transakcji elektronicznych pozwanego banku były właściwe, nie doszłoby do dokonania na rachunku powódki transakcji przeprowadzonych przez nieuprawnione do tego osoby, przy czym jak wynika ze zgromadzonego w sprawie materiału dowodowego, takich przypadków jak powódki w pozwanym Banku było znacznie więcej, co dodatkowo świadczy o tym, że zabezpieczenia stosowane przez pozwanego nie były właściwe. Okolicznością bezsporną było przy tym w sprawie, że powódka padła ofiarą przestępstwa internetowego związanego z usługami bankowości elektronicznej.

Dla skuteczności przeprowadzenia ataku phishingowego, a taki, w świetle zgromadzonego materiału dowodowego w szczególności opinii biegłego, najprawdopodobniej miał miejsce w sprawie, niezbędnym jest wprowadzenie danych logowania na sfałszowanej witrynie banku i umożliwienie w ten sposób przestępcom pozyskania danych do logowania. Podkreślić jednak należy, że do fałszywej bankowości elektronicznej można wejść przypadkowo choćby poprzez serwisy zakupowe. Wprawdzie jak wskazał biegły nie jest jasne, w jaki sposób osoba trzecia uzyskała smsKod przesłany z banku na numer telefonu powódki w dniu zdarzenia, nie mniej nie można tracić z pola widzenia choćby tego, że możliwym jest podpięcie pod system operatora telefonicznego i przechwycenie wysłanego SMS, a jak wskazał biegły pamiętać należy, że działania phishingowe angażują większe grupy przestępcze. W tym miejscu przypomnieć również należy, że w dniu 18 kwietnia 2017 roku również inny klient pozwanego banku (...) zauważył, że na jego rachunku przeprowadzone zostały cztery transakcje płatnicze potwierdzone smsKodem, które zostały wykonane bez jego zgody i wiedzy o ich przeprowadzeniu. Już powyższe wskazuje na przestępczy charakter pozyskania przedmiotowych danych.

Poza wszystkim wskazać należy, że sam biegły nie był w stanie określić ze stuprocentową pewnością w jaki sposób przestępcy pozyskali dane do logowania powódki, nie mniej żaden z dowodów przeprowadzonych w sprawie nie wykazał świadomego bądź celowego działania w tym zakresie samej powódki. Powódka składając zeznania oświadczyła, że nie logowała się na swoje konto w dniu zdarzenia
zaś pozwany nie zdołał obalić jej zeznań w tym zakresie a nie ma żadnych podstaw by odmówić powódce wiarygodności. Nie przeprowadzono żadnego przeciwdowodu na tę okoliczność, przy czym podkreślić należy, że tym nie może być adres IP, z którego dokonano wówczas logowania, a czym uzasadnia swoje stanowisko pozwany, wobec tego, że jak wskazano we wcześniejszej części uzasadnienia adres IP nie jest stały, przydzielony do konkretnego urządzenia, nadto jednocześnie może być przydzielony do ok. 2 tysięcy urządzeń! Podkreślić również należy, że o ile w sprawie bezsporne jest, że powódka padła ofiarą przestępstwa internetowego związanego z usługami bankowości elektronicznej, o tyle brak jest stuprocentowej pewności, co do dokładnego jego przebiegu. Jak wcześniej wskazano jest wiele metod popełniania przestępstw związanych z usługami bankowości elektronicznej, przykładowo związanych z użyciem samej karty bankowej jest około 100 metod ich popełnienia, jak zeznał sam pracownik pozwanego banku. Powołany zaś w sprawie biegły w swojej opinii wskazał jedynie, że najprawdopodobniej powódka padła ofiarą phishignu wskazując jego prawdopodobny przebieg. Jedynie na marginesie wskazać należy, że nawet gdyby przyjąć, że to powódka w dniu zdarzenia logowała się na fałszywej stronie banku, czego jednak w sprawie nie ustalono i nie wykazano, to zrobiła to w sposób niezamierzony i nieświadomy. Podkreślić jeszcze raz należy, że pozwany nie dostarczył jakichkolwiek dowodów, które uzasadniałyby przyjęcie odmiennego wniosku.

W efekcie przestępnego pozyskania danych identyfikacyjnych powódki przez osoby nieuprawnione o nieustalonej tożsamości, osoby te uzyskały możliwość zalogowania się do konta powódki i wykonania czterech przelewów. Choć czynności te z punktu widzenia systemu informatycznego Banku były przeprowadzone formalnie poprawnie, okoliczność ta jest jednak absolutnie niewystarczająca do uznania, że sporne transakcje zostały autoryzowane przez powódkę.

Przypomnienia wymaga, że w myśl art. 40 ust. 1 ustawy, transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji w sposób przewidziany w umowie między płatnikiem a jego dostawcą. W realiach niniejszej sprawy nie budzi wątpliwości, że powódka takiej zgody nie tylko nie wyraziła ale nawet nie miała świadomości jej przeprowadzenia, za czym przemawia również fakt, że po wykryciu kradzieży M. K. niezwłocznie powiadomiła pozwany Bank oraz złożyła zawiadomienie o popełnieniu przestępstwa na Policji, a zatem wypełniła obowiązki nałożone na niej mocą art. 44 ust. 1 ustawy.

Podkreślić jeszcze raz należy, że zgodnie z art. 45 ustawy, 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. Jego powinnością jest bowiem udowodnienie także innych okoliczności, które wykażą autoryzację transakcji przez płatnika, czy też takich, które pozwalają przyjąć, że posiadacz rachunku bądź 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. Powinności tej pozwany nie zdołał sprostać.

W realiach rozpoznawanej sprawy powódce nie sposób przypisać zgody ani woli podjęcia czynności zmierzających do przeprowadzenia spornych transakcji płatniczych przy użyciu posiadanych przez nią instrumentów płatniczych, które to okoliczności świadczyłyby o autoryzowaniu przez nią transakcji. Sąd nie znajduje także podstaw, aby powódce przypisać umyślne doprowadzenie do nieautoryzowanych transakcji płatniczych. O ich dokonaniu powzięła ona wiedzę niemal 3 tygodnie później, co już samo w sobie oznacza, że zostały one przeprowadzone bez jej wiedzy.

Zdaniem Sądu powódce nie można również przypisać rażącego niedbalstwa w naruszeniu obowiązków, wynikających z art. 42 ustawy. O czym była mowa wyżej, brak jest dowodu wykazującego w sposób nie budzący wątpliwości w jaki sposób

i w jakiej dacie nastąpiło udostępnienie osobom nieuprawnionym danych do logowania nie mniej w świetle zebranego w sprawie materiału dowodowego nie sposób przyjąć by to nastąpiło w okolicznościach świadczących niedbalstwie z strony powódki. Jak wynika ze zgromadzonego w sprawie materiału dowodowego, w szczególności z opinii biegłego sądowego do pozyskania danych logowania przez przestępców może dojść wskutek przypadkowego wejścia na fałszywą stronę banku, choćby przez przypadkowe wpisanie niepoprawnego adresu, czy też za pośrednictwem serwisów zakupowych, z których korzystała powódka, a co przecież nie jest co oczywiste zabronione. Do wykonania ataku nie jest konieczne użycie złośliwego oprogramowania, a jedynie podrobienie witryny banku, przy czym sprawdzenie certyfikatu bezpieczeństwa banku wymaga wiedzy specjalistycznej i nie jest zadaniem łatwym. Pamiętać również należy, że w dacie zdarzenia powódka była osobą małoletnią z pewnością nieposiadającą specjalistycznej wiedzy we wskazanym zakresie, przy czym bank musiał mieć świadomość powyższego i godzić się na to skoro umowa bankowa była na rzecz małoletniej osoby. Nie można również tracić z pola widzenia okoliczności, że w toku prowadzonego postępowania nie udało się ustalić dokładnego sposobu działania osób, które doprowadziły do wyprowadzenia środków pieniężnych zgromadzonych na rachunku bankowym należącym do powódki, a wyłącznie konkretne ustalenia mogłyby stanowić podstawę oceny czy w ogóle a jeśli tak w jakim zakresie – M. K. ewentualnie przyczyniła się do zdarzenia. Jednocześnie w sprawie nie zostało wykazane, iż komputer powódki nie posiadał oryginalnego, aktualnego oprogramowania systemowego /antywirusowego, że był on zainfekowany wirusami, że powódka logowała się z innego, niż zazwyczaj urządzenia, czy wreszcie, że korzystała z niezabezpieczonej, obcej sieci internetowej, czy tego by powódka przekazała komukolwiek dane do logowania. Jednocześnie bezspornym jest, że nie tylko powódka padła ofiarą ataku cyberprzestępców przy pomocy opisanej metody, lecz także inni klienci pozwanego Banku. Sama powódka była przesłuchiwana w sprawie innej kradzieży mającej miejsce na Śląsku, z której środki były przelane na konto docelowe tożsame z kontem, na które przelano również środki powódki, a inny klient banku (...) również 18 kwietnia 2018 roku odkrył, że w podobny sposób jak powódka został pozbawiony swoich środków zgromadzonych na koncie. To wszystko prowadzi do wniosku, że strona internetowa banku, z której potencjalnie mogła korzystać powódka, nie przedstawiała się jako oczywiście fałszywa. Wprawdzie pozwany przesyłał powódce dwukrotnie rok przed zdarzeniem ostrzeżenia o możliwych atakach cyberprzestępców, jednak sam fakt przesłania wiadomości na pocztę e-mail jeszcze niczego nie przesądza; powszechność skutecznie przeprowadzonych ataków phishingowych nie tylko w Polsce, ale i na świecie, oraz ich duża ilość daje przy tym asumpt do wniosku, że mimo ostrzeżeń, jakie niewątpliwie część z ofiar otrzymała, bardzo trudno obronić się przed takim atakiem.

W konsekwencji w ocenie Sądu, powyższe okoliczności w żadnej mierze nie pozwalają na przypisanie powódce rażącego niedbalstwa w wykonywaniu wiążącej
ją z bankiem umowy.

Jedynie na marginesie warto również zauważyć, że judykatura konsekwentnie nie uznaje działania posiadacza rachunku, który udostępnia dane logowania na skutek podstępnego działania osób trzecich, za rażące niedbalstwo. Podanie bowiem loginu i hasła na fałszywej stronie logowania należy uznać za dopuszczalny błąd w obliczu podmienionej strony, trudnej do zweryfikowania w pierwszym momencie. (por. m.in. wyrok SO w Bielsku-Białej z dnia 6 grudnia 2018 roku, I C 338/17, L.; wyrok SO w Łodzi z dnia 15 października 2018 roku, II C 73/16, L.; wyrok SO w Krakowie z dnia 3 lipca 2018 roku, II Ca 452/18, L.; wyrok SA w Warszawie z dnia 24 maja 2018 roku, VI ACa 217/17, MonPrBank. 2020/6/15; wyrok SO w Łodzi z dnia 10 kwietnia 2017 roku, III Ca 43/17, L.; wyrok SO w Warszawie z dnia 19 grudnia 2016 roku, I C 229/15, L.).

W sprawie, o czym wcześniej była mowa, nie zostało również wykazane, aby powódka udostępniła dane logowania innym osobom, w tym swoim rodzicom. Powyższe, wbrew twierdzeniom pozwanego, nie wynika z zeznań K. R., czy P. K., co do zeznań których Sąd nie znajduje podstaw, aby je dezawuować. Ojciec powódki wprost zaprzeczył, aby logował się na konto dodając, że nie znał hasła, K. R. zeznała zaś „ja ani mój mąż nigdy nie zaglądaliśmy na to konto". Powyższe potwierdziła M. K. akcentując, iż nie przekazywała danych rodzicom. Co się zaś tyczy wpisania smsKodu przypomnienia wymaga, że powódka wyjaśniła, że wiadomość sms odczytała dopiero w banku,
że w tym czasie dostawała dużo sms od banku z ofertami jego produktów, a biorąc pod uwagę, że była ona wówczas osobą bardzo młodą, nie budzą wątpliwości Sądu jej zeznania w tym zakresie, nadto pozwany nie wykazał, że było

inaczej. Relewantne znaczenie ma w tym przypadku opinia biegłego sądowego, w której treści wprost wskazano, iż nie jest jasne, w jaki sposób osoba trzecia uzyskała smsKod przesłany z banku do powódki. Tak naprawdę wszelkie twierdzenia w tym zakresie wywodzone przez pozwanego mają postać wyłącznie supozycji, która nie poddaje się weryfikacji w świetle zaoferowanych przez pozwanego dowodów.

Strona pozwana wywodziła również, iż powódka znacznie wcześniej powzięła wiedzę o kradzieży, a mimo to zwlekała z poinformowaniem banku do dnia 5 maja 2017 roku. W ocenie Sądu również to twierdzenie nie zostało dowiedzione. Pozwany opiera swoje przekonanie odnośnie wiedzy powódki na danych logowania z dnia 18 kwietnia 2017 roku, które nastąpiło z tej samej puli adresów co logowanie
m.in. w dniu 5 maja 2017 roku, co do którego brak jest wątpliwości, iż zostało wykonane przez powódkę, a także na sprawdzeniu w dniu 18 kwietnia 2017 roku historii rachunku bankowego. Rzecz jednak w tym, że w powyższym zakresie dysponujemy wyłącznie pulą adresów IP, która – co wynika z ustalonego stanu faktycznego oraz pisemnych oświadczeń firm (...) i P. – niczego nie dowodzi. Obaj dostawcy Internetu zgodnie wyjaśnili, że udostępniane przez nich adresy IP nie są przypisane do konkretnych użytkowników, a są przyznawane losowo w jednym czasie do połączeń z Internetem wielu użytkownikom. Firma (...) wskazała przy tym, iż mowa tu o nawet 2 tysiącach użytkowników jednocześnie. Uwzględniając okoliczność, że w omawianej kwestii mamy do czynienia nie tyle z tym samym adresem IP, ale z adresem wchodzącym w skład jednej puli adresów, przyjęcie wyłącznie na podstawie faktu, iż z adresu tego nastąpiło logowanie na konto powódki w dniu 18 kwietnia 2017 roku, że to powódka dokonała tego logowania, jest całkowicie nieuprawnione. Jednocześnie z uwagi na upływ czasu nie można było uzyskać informacji, które być może pozwoliłyby powiązać poszczególne logowania z miejscem, czy też urządzeniem. Wedle twierdzeń pozwanego zasady logicznego rozumowania i doświadczenia życiowego wskazują, iż musiała być to powódka i nie mogli być to przestępcy, pozwany nie rozwija jednak tej myśli, nie wiadomo zatem jaki jest tok jego rozumowania. Pozwany a priori eliminuje jedynie możliwość aktywności przestępców. Powyższego nie sposób jednak wykluczyć, mogło się zdarzyć, że przestępcy chcieli sprawdzić, czy powódka wykryła kradzież, czy rachunek jest czynny, czy być może pojawiły się na nim nowe środki. Pamiętać bowiem należy, że powódka kategorycznie i konsekwentnie twierdziła, że wiedzę o kradzieży powzięła dopiero w dniu 5 maja 2017 roku a jej zeznania w tym zakresie nie zostały w żadnej mierze skutecznie podważone przez pozwanego. Jednocześnie pozwany wydaje się pomijać ocenę racjonalności rzekomego zachowania powódki. Tymczasem zdaniem Sądu, zachowanie M. K., która miałaby się zalogować dwukrotnie na rachunek bankowy w tak krótkim odstępie czasu, w sytuacji, w której rachunek na przestrzeni wielu miesięcy był właściwie nieużywany, a następnie ukryć fakt kradzieży, byłoby pozbawione rzeczonej racjonalności. Powódka, choć małoletnia, musiała sobie przecież zdawać sprawę z tego, że dokonanie takiej czynności pozostawia trwały ślad w systemie bankowym. Równie niewytłumaczalne byłoby czekanie przez ponad dwa tygodnie z ujawnieniem zdarzenia. Zaznaczenia wymaga, że po dokonaniu kradzieży środków saldo na rachunku bankowym było dodatnie (wynosiło 6.664,45 zł), a w dniu 20 kwietnia 2017 roku rachunek został zasilony kwotą 10.000 zł. Innymi słowy powódka posiadała wystarczające środki do pokrycia kosztu zakupu biletu, ergo ujawnienie kradzieży akurat w dniu 5 maja 2017 roku nie było konieczne. Sąd dostrzega wprawdzie, że relacja powódki i K. R. nie jest zgodna odnośnie tego, czy to powódka zalogowała się na konto i po ujrzeniu salda zawołała matkę, czy też powódka logowała się w obecności matki i obie kobiety dostrzegły kradzież, ale okoliczność ta pozostaje zupełnie bez znaczenia dla oceny zasadności powództwa, nadto zauważyć należy, że gdyby powódka chciała ukryć kradzież nie prosiłaby matki o pomoc. Dlatego też, wobec braku dowodów przeciwnych, Sąd doszedł do wniosku, że M. K. odkryła kradzież środków dopiero w dniu 5 maja 2017 roku jak kategorycznie i konsekwentnie zeznawała. Jej zeznania na tę okoliczność są logiczne i spójne, korespondują z relacją jej rodziców, ponadto znajdują oparcie w zasadach doświadczenia życiowego. Powtórzenia wymaga, że zebrany w sprawie materiał dowodowy pozwala jedynie na przyjęcie, iż w dniu 18 kwietnia 2017 roku miało dwukrotnie miejsce logowanie na rachunek bankowy powódki, które nastąpiło z tej samej puli adresów co m.in. logowanie w dniu 5 maja 2017 roku. Każdy dalej idący wniosek pozwanego jest wyłącznie domysłem, niepopartym jakimikolwiek dowodem. Powtórzenia wymaga, że pozwany, jako dostawca usługi, ma obowiązek udowodnić, że transakcja płatnicza została przez użytkownika autoryzowana albo że płatnik umyślnie albo wskutek rażącego niedbalstwa doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie albo wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42. Nie wystarczy zatem, że dostawca usługi przedstawi

możliwą wersję zdarzeń. Dostawca usługi musi udowodnić, że zaistniały okoliczności z art. 45 ust. 2, czego w przedmiotowej sprawie nie uczynił.

Pamiętać również należy, że zobowiązanie banku względem posiadacza rachunku kształtuje także regulacja zawarta w art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997 roku Prawo bankowe, który stanowi że bank dokłada szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Zapewnienie zaś bezpieczeństwa depozytów jest jednym z najistotniejszych obowiązków banku, a sposób jego wykonywania jest najbardziej wymierną podstawą oceny jego wiarygodności. W tym zakresie na banku zawsze spoczywa obowiązek dołożenia wszelkich starań, bowiem profesjonalny charakter jego działalności wymaga stosowania podwyższonego miernika staranności przy wykonywaniu zobowiązań. W tym kontekście zwrócić należy uwagę, że pozwany wykonał dyspozycję dodania zaufanego odbiorcy o nazwie „vcbxcvbxvcbvxcbxc", która prima facie winna wzbudzić jego podejrzenia. Wprawdzie biegły sądowy nie był w stanie odpowiedzieć na pytanie, czy utworzenie użytkownika o przytoczonej nazwie powinno być wychwycone, jako anomalia, to jednocześnie wyjaśnił, że bank powinien przyjmować, że każdy komunikat pochodzący od użytkownika może być obciążony złośliwą treścią. Dlatego też każdy komunikat przychodzący do banku z zewnątrz powinien być traktowany ze szczególną starannością, m.in. w celu oddzielenia potencjalnie złośliwych treści od właściwego komunikatu.

Na koniec przypomnienia wymaga, że zgodnie z treścią art. 8 ust. 1 i 2 ustawy postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego nie mogą być mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy, chyba że ustawa stanowi inaczej. Postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy są nieważne zamiast nich stosuje się odpowiednie przepisy ustawy.

Zgodnie z art. 46 ust. 1 ustawy, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. Jeżeli jednak płatnik doprowadził do nieautoryzowanej transakcji umyślnie
albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42, odpowiada on za nieautoryzowane transakcje płatnicze w pełnej wysokości (art. 46 ust. 3). Jak zaznaczono powyżej, przepis ten nie może mieć zastosowania w niniejszej sprawie wobec braku podstaw do przypisania powódce umyślności czy rażącego niedbalstwa.

W niniejszej sprawie brak jest również podstaw do zastosowania regulacji zawartej w art. 46 ust. 2 ustawy, stanowiącej że jeżeli nieautoryzowana transakcja jest skutkiem nieuprawnionego użycia instrumentu płatniczego w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2, płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 150 euro. Pozwany nie zdołał wykazać, że powódka obowiązki te naruszyła. Wręcz odwrotnie, zebrany w sprawie materiał dowodowy pozwala na przyjęcie, że M. K., jako klientka banku nie naruszyła tych obowiązków, o czym świadczą powołane powyżej okoliczności. Bezzasadne jest zatem twierdzenie pozwanego, że powódka przyczyniła się do powstania szkody.

Mając powyższe na uwadze Sąd zasądził od pozwanego na rzecz powódki kwotę 19.963 zł z ustawowymi odsetkami za opóźnienie od dnia 6 czerwca 2017 roku do dnia zapłaty. Ponieważ pozwany dopuścił się opóźnienia w zwrocie zasądzonej wyrokiem kwoty, powódce należały się odsetki w wysokości ustawowej zgodnie
z art. 481 § 1 i 2 k.c. W myśl cytowanego już art. 46 ust. 1 ustawy, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej „niezwłocznie". Pojęcie to ma charakter niedookreślony i winno zostać wypełnione treścią w odniesieniu do konkretnych okoliczności sprawy. W ocenie Sądu wskazany przez powódkę w uzasadnieniu 30-dniowy termin liczony od daty wniesienia reklamacji (tj. od dnia 5 maja 2017 roku) uznać należy za odpowiedni, stąd też roszczenie odsetkowe było zasadne w całości.

O kosztach procesu orzeczono na podstawie art. 98 k.p.c. zasądzając od pozwanego na rzecz powódki kwotę 3.917 zł, na którą złożyły się: opłata sądowa od pozwu – 300 zł, wynagrodzenie pełnomocnika w stawce minimalnej – 3.600 zł oraz opłata skarbowa od pełnomocnictwa – 17 zł. Ponadto na podstawie art. 113 ust. 1 ustawy o kosztach sądowych w sprawach cywilnych w zw. z art. 98 k.p.c. Sąd nakazał pobrać od pozwanego na rzecz Skarbu Państwa – Sądu Rejonowego dla Łodzi-Widzewa w Łodzi kwotę 234,71 zł tytułem nieuiszczonych kosztów sądowych.