Sygn. akt: I C 277/20

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 28 czerwca 2022 r.

Sąd Rejonowy w Gdyni I Wydział Cywilny

w składzie następującym:

Przewodniczący: SSR Joanna Jank

Protokolant: starszy sekretarz sądowy Katarzyna Pietkiewicz

po rozpoznaniu na rozprawie w dniu 31 maja 2022 r. w G.

sprawy z powództwa ***L. B.***

przeciwko Spółdzielczej Kasie Oszczędnościowo-Kredytowej im. F. S. w G.

o zapłatę

1.oddala powództwo,

2.zasądza od powoda na rzecz pozwanego kwotę 6617 zł (sześć tysięcy sześćset siedemnaście złotych) z tytułu zwrotu kosztów postępowania,

3.nakazuje ściągnąć od powoda na rzecz Skarbu Państwa – Sądu Rejonowego w Gdyni kwotę 2024 zł (dwa tysiące dwadzieścia cztery złote) z tytułu zwrotu wydatków wyłożonych tymczasowo przez Skarb Państwa.

Sygnatura akt I C 277/20

UZASADNIENIE

Powód L. B. wniósł pozew przeciwko Spółdzielczej Kasie Oszczędnościowo – Kredytowej im. F. S. z siedzibą w G. o zapłatę kwoty 45.000 zł wraz z odsetkami ustawowymi za opóźnienie od dnia 16 sierpnia 2018r. do dnia zapłaty.

W uzasadnieniu pozwu powód podniósł, że pozwany prowadzi na jego rzecz rachunek bankowy, a w dniu 7 sierpnia 2018r. w wyniku operacji nr 1675422355 rachunek ten został obciążony kwotą 45.000 zł, która stanowiła nieautoryzowaną przez powoda transakcję na rachunek nr (...). Przelew został wykonany na rzecz odbiorcy o nazwisku S. L.. Powód tego przelewu nie wykonał, nie autoryzował i dowiedział się o nim po zalogowaniu na konto w dniu 10 sierpnia 2018r. Mimo zgłoszenia ww. zdarzenia pozwanemu, (...) odmówiło zwrotu środków. Powód wskazuje, że nie zna odbiorcy przelewu, nie posiada IP, z którego zostało zrealizowane polecenie przelewu, a w dniu jego wykonania przebywał w Polsce i nie korzystał z rachunku. O zdarzeniu powód zawiadomił organy ścigania, lecz dochodzenie zostało umorzone z powodu nieustalenia sprawców. Jako podstawę roszczenia powód wskazał przepis art. 46 ust. 1 ustawy o usługach płatniczych. Powód zaprzeczył przy tym sugestiom pozwanego, jakoby mógł umyślnie lub wskutek rażącego niedbalstwa podać osobom trzecim jakiekolwiek unikatowe dane (login, hasło, wiadomość sms) jako nieudowodnionym i całkowicie gołosłownym. Powód dochował należytej staranności w korzystaniu z serwisu transakcyjnego, był wyłącznym użytkownikiem loginu i hasła do konta internetowego i nie udostępniał tych danych osobom trzecim.

(pozew, k. 3-9)

Pozwany wniósł o oddalenie powództwa w całości. Jak wskazał, system bankowości elektronicznej w dniu wykonania spornych operacji działał prawidłowo i nie był poddany atakom hackerskim, a stan zabezpieczeń był prawidłowy i skuteczny. Z przeprowadzonego przez pozwaną wewnętrznego postępowania wynika, że do realizacji przedmiotowej transakcji doszło wskutek zainfekowania złośliwym oprogramowaniem stacji roboczej (komputera lub telefonu) powoda, z których logował się na stronę internetową pozwanej. Na podstawie analizy historii rachunku wynika, że w dniu 23 lipca 2018r. powód wykonał operację „opłata za energię", a kwota przelewu i nr rachunku różniły się od dotychczasowych przelewów związanych z opłatami za energię. W dniu 6 sierpnia 2018r. została wykonana operacja logowania z urządzenia iPhone oraz adresu IP, które nigdy wcześniej i później nie były wykorzystywane przez powoda. Zdarzenia te mogły być momentem, w którym zostało przejęte hasło powoda. Historia logowań i operacji na rachunku w dniach 23 lipca – 10 sierpnia 2018r. wskazuje, że osoba zlecająca przedmiotowe polecenie przelewu znała indywidualne dane logowania do systemu bankowości elektronicznej, była w posiadaniu wiadomości przesyłanych na nr telefonu powoda, co umożliwiało zlecenie, a następnie autoryzację dyspozycji. Zdaniem pozwanego działania hackerów były możliwe najprawdopodobniej z uwagi na otworzenie przez powoda podejrzanego maila, co mogło doprowadzić do zainstalowania oprogramowania szpiegowskiego, które zainfekowało urządzenie. Powód zatem przyczynił się w całości do powstania szkody, co przejawiało się niezachowaniem przez niego należytej staranności w ochronie swoich danych i co doprowadziło do udostępnienia ich osobom nieuprawnionym. Powód swoim działaniem umożliwił przestępcom kradzież środków pieniężnych ze swojego rachunku, gdyż zatwierdził kodem sms przelew na kwotę 5,09 zł, co mogło skutkować przechwyceniem danych. Nie nastąpiło natomiast przełamanie zabezpieczeń systemu bankowości elektronicznej.

(odpowiedź na pozew, k. 51-59)

Sąd ustalił następujący stan faktyczny:

Powód L. B. jest posiadaczem rachunku bankowego nr (...) prowadzonego przez pozwaną Spółdzielczą Kasę Oszczędnościowo – Kredytową im. F. S. z siedzibą w G.. Pełnomocnikiem upoważnionym do korzystania z tego rachunku była żona powoda G. B.. Na podstawie zawartej z pozwanym w dniu 27 października 2010 roku umowy powód korzysta z usługi bankowości elektronicznej e-skok.

(dowód: umowa o świadczenie usługi e-skok z dnia 27 października 2010r., k. 73-74, zeznania świadka G. B., płyta CD k. 117)

Zgodnie z § 7 ust. 3 Regulaminu świadczenia usługi bankowości elektronicznej e-skok przez (...) im. (...) – obowiązującego od dnia 2 stycznia 2018 roku – użytkownik z chwilą otrzymania dostępu do usługi bankowości elektronicznej e-skok podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych zabezpieczeń usługi bankowości elektronicznej e-skok. Użytkownik zobowiązany jest m.in. do:

- przechowywania i ochrony loginu, hasła i jednorazowych haseł sms, z zachowaniem należytej staranności,

- nieprzechowywania loginu razem z hasłem,

- nieudostępniania loginu, hasła i jednorazowych haseł sms osobom nieuprawnionym,

- zmiany hasła w przypadku jego utraty lub podejrzenia jego ujawnienia osobom nieuprawnionym.

Zgodnie z § 7 ust. 4 Regulaminu odpowiedzialność za skutki ujawnienia loginu, hasła lub jednorazowych haseł sms osobom nieuprawnionym ponosi wyłącznie użytkownik.

(dowód: Regulamin świadczenia usługi bankowości elektronicznej e-skok przez (...) im. (...), k. 77-81)

Przed czerwcem 2015r. powód dokonał zmiany hasła logowania do serwisu bankowości elektronicznej. Natomiast, w dniu 18 czerwca 2018r. dokonał zmiany sposobu autoryzacji operacji poprzez wybór haseł jednorazowych sms.

(dowód: raport logów, k. 65-72)

(...) S.A. z siedzibą w G. wystawił na rzecz powoda fakturę VAT nr (...) na kwotę 5,09 zł z terminem płatności do dnia 30 lipca 2018r. z tytułu rozliczenia zużycia energii elektrycznej za okres od 30 czerwca do 10 lipca 2018r. dotyczące lokalu przy ul. (...) 8/12 w G.. Na fakturze wskazano nr konta odbiorcy: (...).

(dowód: pismo (...) S.A. z dnia 29 lipca 2020r. k. 119 wraz z fakturą VAT nr (...), k. 120-121)

W dniu 23 lipca 2018r. godz. 6:56:31 – 07:02:29 powód wykonał operację „opłata za energię" na kwotę 5,09 zł. Operacja została wykonana przy użyciu IP powoda 89.71.42.120. Dokonując płatności, początkowo powód zamierzał skorzystać z przelewu zdefiniowanego, lecz ostatecznie wykonał przelew jednorazowy. Przedmiotowy przelew został wykonany na nr konta (...). Opis przelewu: „za m. 12 (...).

(dowód: raport logów, k. 65-72)

Ponowne logowanie do serwisu bankowości elektronicznej z IP powoda 89.71.42.120 nastąpiło w dniu 23 lipca 2018r. w godzinach 07:04:00-07:07:51.

(dowód: raport logów, k. 65-72)

W dniu 6 sierpnia 2018r. godz. 13:40:48-13:43:04 nastąpiło za pośrednictwem operatora Polkomtel ((...)) logowanie i wylogowanie do serwisu bankowości elektronicznej z urządzenia iPhone i adresu IP 5.60.224.106.

(dowód: raport logów, k. 65-72)

Następnie, tego samego dnia o godz. 13:46:22 nastąpiło logowanie do serwisu bankowości elektronicznej powoda z IP 94.224.139.56 (operator Telenet, Belgia). Osoba dokonująca logowania weszła na stronę rachunków bieżących, wywołała stronę przelewów jednorazowych, następnie stronę przelewów zdefiniowanych, wybrała nowy przelew zdefiniowany, po czym ustanowiła nowy szablon przelewu zdefiniowanego o nazwie L. M., nr rachunku odbiorcy ((...)), nazwa odbiorcy (S. L.), szczegóły transakcji – („z/ 4r9.49"), co nastąpiło o godz. 13:49:49. Powyższa operacja była autoryzowana jednorazowym hasłem sms wysłanym na nr telefonu powoda 601 652 281, a szablon był z opcją „trusted" (zaufany, co oznacza, że transakcje przy użyciu tego szablonu nie wymagały autoryzacji). Następnie, nastąpiło kilkukrotne wywołanie strony przelewy jednorazowe, rachunki bieżące, przelewy zdefiniowane, a o godz. 13:52:29 nastąpiło wylogowanie z serwisu.

(dowód: raport logów, k. 65-72)

W dniu 6 sierpnia 2018r. o godz. 15:15:04 nastąpiło ponowne logowanie z IP 94.224.139.56 (Belgia) do serwisu bankowości elektronicznej powoda, po czym nastąpiło wywołanie listy rachunków bieżących, otwarcie zakładki z przelewami jednorazowymi, a następnie listy odbiorców zdefiniowanych, otwarcie wcześniej zdefiniowanego szablonu odbiorcy zdefiniowanego L. M., a o godz. 15:16:27 nastąpiło wylogowanie.

(dowód: raport logów, k. 65-72)

Kolejne logowanie, tym razem z IP 84.195.55.57 (Belgia) miało miejsce w dniu 7 sierpnia 2018r. o godz. 07:40:04. Osoba dokonująca logowania wywołała stronę z listą rachunków bieżących, stronę przelewów jednorazowych, stronę z listą odbiorców zdefiniowanych, po czym wybrała z listy szablon L. M., następnie ponownie została wywołana strona przelewów jednorazowych, lista rachunków bieżących, strona przelewów jednorazowych, lista odbiorców zdefiniowanych, aż wreszcie został ponownie wybrany szablon L. M.. O godz. 07:45:16 zostały zatwierdzone wprowadzone parametry przelewu zdefiniowanego (kwota 45.000 zł, zmiana opisu „za m. 12 (...) 10") i zostało zatwierdzone wykonanie przelewu zdefiniowanego o godz. 07:45:21. Operacja została zarejestrowana została pod nr (...). Zatwierdzenie przelewu nie wymagało podania jednorazowego hasła sms.

(dowód: potwierdzenie wykonania operacji, k. 13, raport logów, k. 65-72)

W czasie tej samej sesji o godz. 07:46:12 osoba zalogowana z IP 84.195.55.57 weszła na stronę zmiany hasła (nie dokonując jego zmiany), a następnie wielokrotne wchodziła na stronę wywołania o oczekujących zleceniach. W. z serwisu bankowości elektronicznej nastąpiło dopiero o godz. 09.37:44.

(dowód: raport logów, k. 65-72)

W dniu 7 sierpnia 2018r. o godz. 09:37:58 nastąpiło kolejne logowanie z IP 84.195.55.57 (Belgia), a następnie wywołanie strony rachunków bieżących oraz przelewów jednorazowych. O godz. 09:50:02 nastąpiło wylogowanie z serwisu.

(dowód: raport logów, k. 65-72)

W międzyczasie, o godz. 09:49:46 z IP 77.253.201.60 (netia.pl) nastąpiło logowanie do serwisu bankowości elektronicznej z urządzenia mobilnego. Użytkownik wywołał tylko stronę rachunków bieżących, po czym wylogował się o godz. 09.50:02.

(dowód: raport logów, k. 65-72)

W dniu 7 sierpnia 2018r. o godz. 09:50:25 nastąpiło trzykrotne nieudane logowanie z IP 84.195.55.57, a po trzeciej próbie doszło do zablokowanie kanału dostępu (09:51:41).

(dowód: raport logów, k. 65-72)

W dniu 10 sierpnia 2018r. godz. 14:38:01 nastąpiło odblokowanie dostępu do bankowości elektronicznej za pośrednictwem Infolinii.

(dowód: raport logów, k. 65-72)

Po zalogowaniu się do serwisu bankowości elektronicznej w dniu 10 sierpnia 2018r. powód zorientował się, że z jego rachunku wykonano przelew na kwotę 45.000 zł.

(dowód: raport logów, k. 65-72, przesłuchanie powoda, płyta CD k. 117)

W dniu 13 sierpnia 2018r. powód złożył w oddziale (...) pisemną reklamację, wskazując, że w dniu 7 sierpnia 2018r. dokonano z jego rachunku nieautoryzowanego przelewu na kwotę 45.000 zł.

(dowód: reklamacja powoda z dnia 13 sierpnia 2018r., k. 14)

Pismem z dnia 10 września 2018r. pozwany wskazał, że przeprowadzona przez niego analiza nie wykazała naruszenia zabezpieczeń w usłudze bankowości elektronicznej e-skok, lecz z uwagi na fakt, że powód nie zatwierdził ww. polecenia przelewu, (...) zasugerował skierowanie sprawy do organów ścigania w celu przeprowadzenia szczegółowej weryfikacji.

(dowód: pismo pozwanego z dnia 10 września 2018r., k. 15-16)

Pismem z dnia 22 września 2018 roku powód zażądał od pozwanej zwrotu kwoty 45.000 zł, wskazując, że nigdy nie logował się na konto z IP 84.195.55.5 ani nie logował się spoza Polski, nie jest właścicielem rachunku, na który dokonano przelewu.

(dowód: pismo powoda z dnia 22 września 2018r., k. 17)

W odpowiedzi, pismem z dnia 24 października 2018r. pozwany podtrzymał swoje wcześniejsze stanowisko.

(dowód: pismo pozwanego z dnia 24 października 2018r., k. 18)

Postanowieniem z dnia 31 grudnia 2019r. wydanym w sprawie o sygnaturze PR 3Ds 290.2018 prokurator Prokuratury Rejonowej w Gdyni umorzyła dochodzenie w sprawie nieustalonych sprawców, którzy w nieustalonym dniu, nie później niż do 10 sierpnia 2018r. w nieustalonym miejscu działając wspólnie i w porozumieniu z L. S. doprowadzili do niekorzystnego rozporządzeniem mieniem powoda w kwocie 45.000 zł poprzez wpływanie na automatyczne przetwarzanie danych informatycznych rachunku bankowego ww. pokrzywdzonego dokonali przelewu tej kwoty na rachunek bankowy prowadzony dla L. S. celem jej wypłaty tj. o czyn z art. 287 § 1 kk w zb. z art. 286 § 1 kk w zw. z art. 11 § 2 kk – wobec niewykrycia sprawcy.

(dowód: postanowienie prokuratora z dnia 31 grudnia 2019r., k. 38-41)

Powód logował się do serwisu bankowości elektronicznej zazwyczaj z komputera domowego oraz komputera służbowego podłączonego do sieci portowej (także stanowiącego jego własność). Oba komputery powoda nie były zabezpieczone hasłami.

(dowód: zeznania świadka G. B., płyta CD k. 117, przesłuchanie powoda, płyta CD k. 117, 225)

W telefonie jako kontakt został przez powoda dodany wpis o nazwie (...), a w nim został zapisany login powoda do bankowości elektronicznej („ (...)"), natomiast jako notatka do kontaktu zostało zapisane hasło do bankowości elektronicznej („lbartoszewicz"). Ostatnia aktualizacja tego wpisu miała miejsce w dniu 9 lutego 2018r.

Zabezpieczenia transakcji elektronicznych stosowane przez (...) były właściwe. Pozwany nie stosował zabezpieczeń mogących wykryć jednoczesne logowanie się użytkownika z dwóch (lub więcej) urządzeń z kilku krajów, lecz nie było takiego wymogu wynikającego z przepisów prawa.

W lipcu i sierpniu 2018 roku na komputerach powoda było zainstalowane i aktywne legalne oprogramowanie antywirusowe, przy czym na komputerze wykorzystywanym w pracy jedynie program M. D.. Na komputerze stacjonarnym używanym w pracy znajdowało się oprogramowanie szpiegujące umożliwiające dostęp do danych pozwalających na wykonanie transakcji za pośrednictwem systemu bankowości elektronicznej. W dniu 2 sierpnia 2018r. o godz. 2:44:05 powód otrzymał wiadomość e – mail z załącznikiem o nazwie „Fa_ (...).rar", zawierającym złośliwie oprogramowanie typu koń trojański o nazwie „T..V.. (...)". O godz. 9:32:13 powód zapisał otrzymany plik na twardym dysku komputera stacjonarnego w katalogu „Dokumenty\Faktury korygujące". O godz. 12:27:42 w wyniku działania szkodliwego kodu z załącznika, został zdalnie pobrany i uruchomiony złośliwy program (H.. (...).E..4), który został umieszczony na twardym dysku, który mógł się uruchamiać automatycznie ze startem systemu operacyjnego komputera. Program ten mógł doprowadzić do przechwytywania, a także przekazywania danych wrażliwych z komputera oraz z urządzeń, które były do komputera podłączona (np. telefon).

Najprawdopodobniej osoby dokonujące ataku hackerskiego uzyskały zdalny dostęp do zawartości telefonu powoda lub przejęli nad nim całkowitą kontrolę poprzez zainfekowanie urządzenia szkodliwym oprogramowaniem szpiegującym. Jednakże z uwagi na brak przedstawienia do oględzin telefonu powoda nie można tego kategorycznie stwierdzić.

(dowód: pisemna opinia biegłego sądowego z zakresu elektronicznych systemów bankowych i sieci M. W., k. 140-165 wraz z pisemną opinią uzupełniającą, k. 196-199)

Sąd zważył, co następuje:

Powyższy stan faktyczny Sąd ustalił na podstawie dowodów z dokumentów, dowodu z zeznań świadka G. B., dowodu z przesłuchania powoda, a także dowodu z opinii biegłego sądowego z zakresu elektronicznych systemów bankowych i sieci M. W..

Oceniając zebrany w sprawie materiał dowodowy Sąd nie dopatrzył się żadnych podstaw do kwestionowania autentyczności i wiarygodności dowodów z dokumentów prywatnych wymienionych w ustaleniach stanu faktycznego,

w szczególności umowy o świadczenie usług bankowości elektronicznej, korespondencji stron, czy faktury VAT za energię elektryczną. Podkreślić bowiem należy, iż żadna ze stron niniejszego postępowania nie zaprzeczyła prawdziwości tych dokumentów, jak również nie kwestionowała pochodzenia zawartych w nich oświadczeń. Przedmiotowe dokumenty nie noszą bowiem żadnych śladów przerobienia, przerobienia, bądź innej ingerencji. Zatem, przyjąć należało, że są autentyczne, a zawarte w nich oświadczenia pochodzą od osób, które je własnoręcznie podpisały. Za prawdziwe należało również uznać dokumenty stanowiące wydruki z systemów informatycznych pozwanego (raport logów), albowiem - jak wynika z opinii biegłego - załączone do akt sprawy wydruki stanowią odzwierciedlenie danych zapisanych na nośniku elektronicznym.

Niewiele do rozstrzygnięcia sprawy wniosły zeznania świadka G. B., która wskazała, że sama nie korzystała z serwisu bankowości elektronicznej. Zeznania świadka częściowo dotyczyły okoliczności niespornych (np. tego, że powód korzystał z serwisu e-skok za pomocą komputera domowego oraz komputera służbowego). Natomiast, w świetle opinii biegłego, za niewiarygodne należało uznać zeznania świadka co do tego, że powód nigdy nie logował się do systemu bankowości elektronicznej w czasie pobytu na wakacjach czy za granicą. Jak bowiem wskazał biegły w logach systemu bankowego pojawiają się sporadyczne logowania z sieci należącej do Sanatorium w C., hotelu w B., czy nawet z terytorium W. (styczeń 2015).

Za wewnętrznie sprzeczne i w konsekwencji za niewiarygodne należało uznać zeznania powoda. Zważyć należy, iż na rozprawie w dniu 15 września 2020r. L. B. zeznał, że nie zapisywał loginu ani hasła do serwisu bankowości elektronicznej ani też nie logował się do serwisu bankowości elektronicznej z urządzenia iPhone. Jednakże, w wyniku przeprowadzonego przez biegłego badania zawartości dysku twardego komputera okazało się jednak, że na komputerze powoda zapisany jest plik będący bazą danych synchronizacji programu M. O. z urządzeniem iPhone i zawiera on m.in. takie dane jak listy kontaktów czy notatki. Plik ten zawierał pełną książkę adresową, jaką powód posiadał w telefonie. Wśród zapisanych kontaktów znajdował się m.in. wpis o nazwie (...), a w nim został zapisany login powoda do bankowości elektronicznej e-skok, natomiast jako notatka do tego kontaktu została zapisane hasło do serwisu e-skok. Podobnie w książce adresowej były zapisane hasła do serwisów bankowości elektronicznej innych banków. Podczas ponownego przesłuchania powód przyznał, że faktycznie w telefonie miał zapisane login i hasło do bankowości elektronicznej, choć wskazywał, że hasło było zaszyfrowane. Niemniej, treść opinii biegłego przeczy temu, że hasło było w jakikolwiek sposób zabezpieczone szyfrem, skoro biegły odczytał je w niezmienionej postaci. Ponadto, powód zeznał, że zmieniał hasło do bankowości elektronicznej raz na dwa miesiące. Tymczasem, z zebranego materiału dowodowego, w tym raportu logów oraz opinii biegłego, wynika, że ostania zmiana hasła przed atakiem hackerskim w sierpniu 2018 roku miała miejsce przed czerwcem 2015r. (wg twierdzeń pozwanego dokładnie w dniu 9 lutego 2015r., choć załączony raport logów nie obejmuje okresu sprzed czerwca 2015r.). Nadto, w świetle opinii biegłego za niewiarygodne należało uznać zeznania powoda odnośnie posiadania dodatkowej ochrony antywirusowej. Podczas składania zeznań na rozprawie w dniu 15 września 2020r. powód wskazywał, że w czasie pracy w porcie informatycy zainstalowali na jego komputerze program antywirusowy. Tymczasem, biegły wskazał, że na komputerze zainfekowanym koniem trojańskim (a używanym przez powoda w pracy) w dacie ataku hackerskiego był zainstalowany jedynie program W. D., który jest dostarczany wraz z systemem operacyjnym, a więc nie wymagał żadnej dodatkowej instalacji. Wreszcie, za całkowicie niewiarygodne Sąd uznał zeznania powoda dotyczące przyczyn nieudostępniania biegłemu do oględzin telefonu model iPhone. L. B. tłumaczył, że telefon został zagubiony przez jego pięcioletnią wnuczkę podczas zabawy na placu zabaw kilka dni przed wyznaczonym terminem przekazania tego urządzenia do badania biegłemu sądowemu. W ocenie Sądu zbieżność daty rzekomego zagubienia telefonu z datą jego oględzin przez biegłego, świadomość powoda, że na telefonie były zapisane zarówno login, jak i hasło do serwisu bankowości elektronicznej e-skok, a także fakt, że odnośnie zapisywania danych w telefonie powód wcześniej zeznał nieprawdę poddają w wątpliwość przedstawioną przez niego wersję zdarzeń. Zdaniem Sądu powód celowo nie udostępnił biegłemu telefonu do oględzin, aby uniknąć ujawnienia niekorzystnych dla niego faktów. Jednocześnie, wiarygodność przedstawionej przez powoda wersji budzi poważne wątpliwości w świetle zasad doświadczenia życiowego, o czym bliżej mowa będzie w dalszej części niniejszego uzasadnienia. W tych okolicznościach nieudostępnienie biegłemu telefonu do oględzin należało rozpatrywać w kontekście art. 233 § 2 kpc i należało uznać za przeszkodę w przeprowadzeniu dowodu wbrew postanowieniu sądu z dnia 5 marca 2021 roku. Jak

wskazuje się w orzecznictwie w oparciu o wprowadzone w tym przepisie unormowanie, sąd orzekający może uznać za nieudowodnione twierdzenie tej strony, która odmówiła przedstawienia dowodu lub stawiała przeszkody w jego przeprowadzeniu, bądź też przyjąć za prawdziwe twierdzenia strony przeciwnej (por. wyrok SN z 6 lutego 1975 r., II CR 844/74, L.; wyrok SA w Warszawie z dnia 3 kwietnia 2019r., I ACa 121/18, L.).

Natomiast, za wiarygodny i w pełni przydatny do rozstrzygnięcia sprawy dowód Sąd uznał opinię biegłego sądowego z zakresu elektronicznych systemów bankowych i sieci M. W.. W ocenie Sądu opinia złożona przez biegłego została sporządzona w sposób rzetelny, profesjonalny, wnikliwy. Biegły przeanalizował historię logowania do serwisu bankowości elektronicznej, a nadto przeprowadził badanie zawartości twardych dysków z obu komputerów powoda pod kątem obecności wirusów i złośliwego oprogramowania, a także zabezpieczeń antywirusowych, a na wynikach powyższych badań i analiz oparł swoje ustalenia. Wnioski biegłego zostały w sposób należyty uzasadnione, a tok myślowy biegłego nie budzi żadnych wątpliwości Sądu w świetle zasad logicznego rozumowania, wiedzy powszechnej czy doświadczenia życiowego. Ponadto, w opinii uzupełniającej biegły w sposób rzeczowy i przekonujący odniósł się do wszystkich zarzutów zgłoszonych przez stronę powodową, a tym samym obronił opinię.

Przechodząc do rozważań merytorycznych, należy wskazać, iż w niniejszej sprawie powód dochodził od pozwanego zwrotu kwoty 45.000 zł pobranej z rachunku bankowego powoda na skutek nieautoryzowanej transakcji płatniczej, wykonanej bez zgody powoda. Podstawę prawną powództwa stanowił przepis art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011r. o usługach płatniczych (Dz.U. z 2021 r. poz. 1907), zgodnie z którym z zastrzeżeniem art. 44 ust. 2, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika niezwłocznie, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwraca płatnikowi kwotę nieautoryzowanej transakcji płatniczej, z wyjątkiem przypadku gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw. W przypadku gdy płatnik korzysta z rachunku płatniczego, dostawca płatnika przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. Data waluty w odniesieniu do uznania rachunku płatniczego płatnika nie może być późniejsza od daty obciążenia tą kwotą. W myśl natomiast przywołanego art. 44 ust. 2 ustawy o usługach płatniczych jeżeli użytkownik nie dokona powiadomienia, o którym mowa w ust. 1, w terminie 13 miesięcy od dnia obciążenia rachunku płatniczego albo od dnia, w którym transakcja miała być wykonana, roszczenia użytkownika względem dostawcy z tytułu nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcji płatniczych wygasają.

Jak wskazuje się w orzecznictwie ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub, że została wykonana prawidłowo spoczywa na dostawcy. Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez płatnika autoryzowana. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzowanie transakcji przez płatnika albo okoliczności wskazujących na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego obowiązków o których mowa jest w art. 42 ustawy o usługach płatniczych (por. wyrok Sądu Apelacyjnego w Łodzi z dnia 10 marca 2017 r. I ACa 1174/16, L.). Zwrócić przy tym należy uwagę, iż zgodnie z treścią art. 46 ust. 3 ustawy o usługach płatniczych to 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. Stosownie zaś do art. 42 ust. 1 powołanej ustawy użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany:

1) korzystać z instrumentu płatniczego zgodnie z umową ramową oraz

2) zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu.

W myśl ust. 2 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 danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym.

Zważyć należy, iż pozwany bronił się w niniejszej sprawie, wskazując, że powód wskutek rażącego niedbalstwa dopuścił się naruszenia obowiązków o których mowa jest w art. 42 ustawy o usługach płatniczych. Zdaniem pozwanego o rażącym niedbalstwie powoda świadczy przed wszystkim przechowywanie loginów i haseł do bankowości elektronicznej w pamięci przeglądarek internetowych i w książce adresowej telefonu, a w wyniku synchronizacji z programem M. O. także na komputerze. W tym kontekście pozwany powoływał się na zasady bezpieczeństwa w posługiwaniu się bankowością elektroniczną, choćby wskazane w § 7 Regulaminu świadczeń usług bankowości elektronicznej przez (...). Nadto, (...) wskazywał, że o rażącym niedbalstwie powoda świadczy również fakt otwarcia przez niego wiadomości e – mail z dnia 2 sierpnia 2018 roku oraz zapisanie załącznika z rzekomą fakturą korygującą w pamięci komputera, który zawierał złośliwe oprogramowanie.

W ocenie Sądu zarzut pozwanego odnośnie rażącego niedbalstwa powoda należało uznać ostatecznie za uzasadniony, przy czym zawinienie powoda w tak znacznym stopniu nie wynika tylko i wyłącznie z niedochowania przez niego obowiązków związanych z korzystaniem z bankowości elektronicznej w okresie, w którym doszło do nieautoryzowanej transakcji płatniczej, lecz raczej z jego późniejszego postępowania związanego z nieudostępnieniem biegłemu telefonu. W świetle opinii biegłego nie budzi wątpliwości, że powód nie dochował należytej staranności przy zabezpieczeniu swoich danych uwierzytelniających w postaci loginu oraz hasła do serwisu bankowości elektronicznej e-skok. Jak bowiem ustalił biegły na komputerze powoda zapisany jest plik będący bazą danych synchronizacji programu M. O. z urządzeniem iPhone i zawiera on m.in. takie dane jak listy kontaktów czy notatki. Plik ten zawierał pełną książkę adresową, jaką powód posiadał w telefonie. Wśród zapisanych kontaktów znajdował się wpis o nazwie (...), a w nim został zapisany login powoda do bankowości elektronicznej e-skok („ (...)"), natomiast jako notatka do tego kontaktu została zapisane hasło do serwisu e-skok. Niewątpliwie zapisywanie na urządzeniach mobilnych, które mogą zostać przechwycone przez osoby nieuprawnione, danych uwierzytelniających, w szczególności zapisywanie loginu łącznie z hasłem, należy uznać za zachowanie nieostrożne i lekkomyślne. Podobnie, w świetle dochowania reguł należytej staranności negatywnie należało ocenić wybór hasła. Jak ustalił biegły i co ostatecznie przyznał również powód, jego hasło do serwisu bankowości elektronicznej było proste i łatwe do ustalenia, albowiem składało się z pierwszej litery jego imienia oraz z jego nazwiska („lbartoszewicz"). Niemniej, w ocenie Sądu, opisane powyżej uchybienia powoda w należytym zabezpieczeniu danych uwierzytelniających mogą stanowić co najwyżej podstawę do przypisania mu winy nieumyślnej w postaci lekkomyślności, a nie – jak twierdził pozwany – rażącego niedbalstwa.

Jak wynika z opinii biegłego kluczowe dla ustalenia sposobu przechwycenia danych powoda umożliwiających logowanie się do konta bankowego było zbadanie telefonu powoda iPhone. Biegły zwrócił bowiem uwagę, że operacja polegająca na dodaniu przez hackera zdefiniowanego odbiorcy przelewu, co umożliwiło później dokonanie przelewu, wymagała autoryzacji za pomocą kodu jednorazowego sms wysłanego przez bank. Kod jednorazowy został wysłany na nr telefonu powoda. Oznacza to, że albo powód sam dokonał autoryzacji transakcji, albo też hacker musiał taką wiadomość przejąć, co było możliwe w trzech przypadkach tj. poprzez uzyskanie fizycznego dostępu do telefonu powoda lub stałą możliwość podglądu jego ekranu albo przez podszycie się pod numer telefonu powoda, albo poprzez zdalne przejęcie kontroli nad telefonem powoda lub całkowite przekierowanie wszystkich wiadomości, jakie powód otrzymywał poprzez infekcję urządzenia szkodliwym oprogramowaniem. Z uwagi na nieprzedstawienie przez powoda telefonu do oględzin przez biegłego niemożliwe było ustalenie sposobu przechwycenia danych przez osoby dokonujące ataku. W świetle twierdzeń powoda, za mało prawdopodobne biegły uznał dwa pierwsze sposoby przechwycenia kontroli nad telefonem (powód bowiem negował, by stracił kiedykolwiek fizyczną kontrolę nad telefonem, natomiast podszycie się pod numer telefonu powoda wymagałoby wykonania i użycia duplikatu karty SIM, co spowodowałoby automatyczną dezaktywację karty oryginalnej i utratę łączności przez powoda, czemu powód również zaprzeczył). Biegły jedynie postawił hipotezę, że najprawdopodobniej osoby dokonujące ataku hackerskiego uzyskały zdalny dostęp do zawartości telefonu powoda, połączyły się za jego pośrednictwem z bankowością elektroniczną powoda

(vide: pierwsze podejrzane logowanie), a następnie odczytywali wiadomości sms przychodzące z banku, po czym je usuwali. Niemniej, nie sposób powyższej hipotezy w jakikolwiek zweryfikować z przyczyn leżących po stronie powoda, który uniemożliwił wykonanie oględzin telefonu.

W ocenie Sądu działanie powoda polegające nieudostępnieniu telefonu do badania przez biegłego było działaniem celowym mającym na celu uniemożliwienie zbadania zawartości tego urządzenia i ujawnienia niekorzystnych dla powoda faktów. Uniemożliwiło tym samy pozwanemu wykazanie zarzutu rażącego niedbalstwa po stronie powoda. Jak wskazano powyżej, przy okazji oceny dowodów, powód wiedział, że w książce adresowej w telefonie były zapisane dane logowania i zdawał sobie sprawę, że biegły to ujawni. Nadto, powód miał świadomość, że wcześniej przed Sądem zeznał nieprawdę, gdy wskazywał, że nigdy nie zapisywał loginu i hasła. Przedstawiona przez powoda wersja, iż telefon został zagubiony w czasie spaceru przez wnuczkę jest całkowicie niewiarygodna, tym bardziej, że w dacie rzekomej utraty telefonu powód już wiedział, że Sąd uzupełnił postanowienie dowodowe także w zakresie ustalenia czy do przechwycenia danych logowania doszło przy wykorzystaniu iPhone powoda (postanowienie w tym przedmiocie zostało wydane w dniu 5 marca 2021r., natomiast do utraty telefonu miało dojść na przełomie marca i kwietnia 2021r.).

Przedstawiona przez powoda wersja budzi również wątpliwości w świetle zasad doświadczenia życiowego i logicznego rozumowania. Po pierwsze, należy skonstatować, że celem wyjścia na spacer czy na plac zabaw jest zabawa dziecka na świeżym powietrzu, a nie wpatrywanie się przez nie w ekran telefonu, co równie dobrze czynić w domu. Po drugie, należy mieć na uwadze, iż telefon model iPhone jest urządzeniem dość drogim, a podczas jego użytkowania przez kilkuletnie dziecko na spacerze może dojść do różnych nieoczekiwanych zdarzeń, które mogą spowodować uszkodzenie lub zniszczenie telefonu (np. upuszczenie telefonu na chodnik, upadek dziecka z telefonem w ręku etc.). W tym kontekście wydaje się mało prawdopodobne, by powód udostępnił takie urządzenie pięcioletniemu dziecku poza domem, narażając się na zniszczenie wartościowego urządzenia. Jednak – zdaniem Sądu – nawet, gdyby osoba dorosła faktycznie udostępniła takie urządzenie dziecku do zabawy na spacerze, to raczej starałaby się zwracać uwagę na postępowanie dziecka i kontrolować w jaki sposób korzysta ono z tego urządzenia. Jest to tym bardziej uzasadnione, że w telefonie zapisane były dane wrażliwe takie jak login i hasło do serwisu bankowości internetowej. W przypadku utraty telefonu w miejscu publicznym, ogólnodostępnym istnieje całkiem realne zagrożenie, że w posiadanie telefonu wejdą osoby nieuprawnione, które w taki sposób mogą uzyskać dostęp do takich danych. Powyższe uchybienia jest tym bardziej poważne, że wobec niemożności zbadania tego urządzenia przez biegłego nie wiadomo, czy iPhone był należycie zabezpieczony zarówno przed dostępem przez osoby nieuprawnione ((...), znakiem graficznym, hasłem, odciekiem palca), jak też przed złośliwym oprogramowaniem i wirusami (np. czy został zainstalowany na nim program antywirusowy). Niewątpliwie zatem oddanie telefonu kilkuletniemu dziecku do zabawy w miejscu publicznym i następnie utrata urządzenia wobec braku sprawowania należytej kontroli nad korzystaniem z tego urządzenia przez małoletniego (gdyby faktycznie doszło do utraty telefonu w taki sposób, w co – jak wskazano powyżej – Sąd wątpi) stanowiłyby o istotnym zawinieniu powoda w postaci rażącego niedbalstwa.

Zwrócić również należy, że jeżeli strona swoim postępowaniem uniemożliwi lub poważnie utrudni wykazanie okoliczności stronie przeciwnej, na której spoczywał ciężar dowodu (art. 232 kpc), na tę stronę przechodzi ciężar dowodu, że okoliczności takie nie zachodziły (por. A. Góra-Błaszczykowska (red.), Kodeks postępowania cywilnego. Tom I A. Komentarz. Art. 1-42412, Warszawa 2020). Skoro w niniejszym postępowaniu pozwany wniósł o przeprowadzenie dowodu celem ustalenia sposobu przechwycenia danych przez hackerów, a także sposobu zabezpieczenia urządzeń powoda, z których łączył się on z serwisem bankowości elektronicznej (do czego niezbędne były oględziny i badanie urządzeń) celem wykazania rażącego niedbalstwa powoda i uwolnienia się z odpowiedzialności, to uniemożliwienie przeprowadzenia tego dowodu przez powoda, który – jak wyjaśniono powyżej – celowo nie udostępnił telefonu do oględzin biegłemu powoduje, stosownie do powyższego poglądu prawnego, że na niego został przerzucony ciężar dowodu, że nie dopuścił się rażącego niedbalstwa. Tymczasem, tego powód nie zdołał w toku niniejszej sprawy wykazać, albowiem bez oględzin i zbadania telefonu nie sposób ustalić w jaki sposób osoby dokonujące ataku hackerskiego przechwyciły dane powoda umożliwiające logowanie się do konta bankowego i czy urządzenie to było należycie zabezpieczone przed takim atakiem. Zdaniem Sądu całokształt okoliczności sprawy, w tym nieprzedstawienie iPhone'a do oględzin, a tym samym uniemożliwienie przeprowadzenia dowodu i ustalenia, czy

za jego pośrednictwem doszło do przechwycenia danych powoda umożliwiających logowanie się do konta bankowego, zapisanie w książce adresowej tego telefonu danych logowania, składanie przez powoda nieprawdziwych zeznań odnośnie zabezpieczenia danych, świadczy o tym, że powód zmierzał do ukrycia swojego rażącego niedbalstwa.

Mając powyższe na uwadze, na podstawie art. 46 ust. 1 i art. 42 ustawy o usługach płatniczych a contrario, Sąd powództwo oddalił.

O kosztach procesu Sąd orzekł na podstawie art. 98 kpc koc i zgodnie z zasadą odpowiedzialności za wynik sprawy, zasądził na rzecz pozwanego kwotę 6.617 zł, na co składała się opłata za czynności fachowego pełnomocnika w stawce minimalnej (3.600 zł), zaliczka na poczet opinii biegłego (3.000 zł) oraz opłata skarbowa od pełnomocnictwa (17 zł).

Nadto, na art. 98 kpc w zw. art. 5 ust. 3, art. 8 ust.1 i art. 83 i 113 ust. 1 ustawy o kosztach sądowych w sprawach cywilnych Sąd nakazał ściągnąć od powoda na rzecz Sądu Rejonowego – Skarbu Państwa w G. nieuiszczone koszty wynagrodzenia biegłego, które zostały tymczasowo wypłacone ze Skarbu Państwa w kwocie 2.024 zł.