Sygn. akt ***XXVII Ca 1352/21***

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 11 sierpnia 2021 r.

Sąd Okręgowy w Warszawie XXVII Wydział Cywilny Odwoławczy w składzie:

Przewodniczący:	***Sędzia Katarzyna Małysa***

po rozpoznaniu w dniu 11 sierpnia 2021 r. w Warszawie

na posiedzeniu niejawnym

sprawy z powództwa ***B. R.***

przeciwko ***(...) Bankowi (...) Spółce Akcyjnej z siedzibą w W.***

o zapłatę

na skutek apelacji powoda

od wyroku Sądu Rejonowego dla Warszawy Mokotowa w W.

z dnia 17 marca 2021 r., sygn. akt II C 819/20

1. zmienia zaskarżony wyrok w ten sposób, że zasądza od (...) Banku (...) Spółki Akcyjnej z siedzibą w W. na rzecz B. R. kwotę 45 000 (czterdzieści pięć tysięcy) złotych wraz z ustawowymi odsetkami za opóźnienie od dnia 10 września 2019 r. do dnia zapłaty oraz kwotę 4 634 (cztery tysiące sześćset trzydzieści cztery) złote tytułem zwrotu kosztów procesu,

2. zasądza od (...) Banku (...) Spółki Akcyjnej z siedzibą w W. na rzecz B. R. kwotę 2 800 (dwa tysiące osiemset) złotych tytułem zwrotu kosztów procesu w instancji odwoławczej.

Sygn. akt: XXVII Ca 1352/21

UZASADNIENIE

Pozwem z dnia 28 lutego 2020 r. B. R. wniósł o zasądzenie od (...) Bank (...) Spółki Akcyjnej z siedzibą w W. kwoty 45.000 zł wraz z odsetkami ustawowymi za opóźnienie od dnia 10 września 2019 r. do dnia zapłaty. Nadto wniósł o zasądzenie zwrotu kosztów procesu, w tym zwrotu kosztów zastępstwa procesowego według norm przepisanych, wraz z odsetkami ustawowymi za opóźnienie.

W odpowiedzi na pozew pozwany wniósł o oddalenie powództwa w całości oraz zasądzenie od powoda na rzecz pozwanego zwrotu kosztów procesu, w tym kosztów zastępstwa procesowego według norm przepisanych.

Wyrokiem z dnia 17 marca 2021 r. Sąd Rejonowy dla Warszawy Mokotowa w W. oddalił powództwo i orzekł o kosztach procesu.

W pisemnym uzasadnieniu wyroku Sąd Rejonowy wskazał na następujące ustalenia i motywy swojego rozstrzygnięcia.

W dniu 27 lutego 2019 r. powód zawarł z (...) Bank (...) Spółką Akcyjną z siedzibą w W. umowę o prowadzenie bankowego rachunku oszczędnościowo-rozliczeniowego (...) o nr (...). W ramach tej umowy powód korzystał z usług bankowości elektronicznej. Ponadto otwarty został dla powoda rachunek oszczędnościowy o nr (...) skorelowany z rachunkiem oszczędnościowo-rozliczeniowym.

W dniu 08 września 2019 r. powód dostrzegł w historii rachunków bankowych transakcje, których nie zlecał. Były to następujące przelewy z dnia 29 sierpnia 2019 r.:

1. z rachunku o nr (...) należącego do powoda na rachunek o nr (...) należący do nieznanego powodowi odbiorcy o danych S. M. na kwotę 21.500 zł,

2. z rachunku o nr (...) należącego do powoda na rachunek powoda o nr (...) na kwotę 23.500 zł,

3. z rachunku o nr (...) należącego do powoda na rachunek o nr (...) należący do nieznanego powodowi odbiorcy o danych S. M. na kwotę 23.500 zł.

Dostęp do rachunków bankowych powoda posiadał wyłącznie powód. Logowania następowały wyłącznie przy użyciu sprzętu posiadającego legalne oprogramowanie, który wyposażony był w program antywirusowy. Żadne dane wymagane do uzyskania dostępu do bankowości internetowej powoda np. hasło lub login, nie były zapisane w pamięci przeglądarki internetowej. Ponadto powód nie zapisywał ich na żadnych nośnikach.

Logowanie, które nastąpiło na rachunki bankowe powoda w dniu 29 sierpnia 2019 r. o godzinie 23:34, w wyniku którego doszło następnie do nieautoryzowanych przelewów, nastąpiło z innego adresu IP niż adres powoda. Do zdarzenia doszło w wyniku tzw. phishingu. Jest to forma oszustwa, polegająca na podszyciu się przez przestępców pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji typu np. dane do logowania lub dane karty kredytowej, bądź też zainfekowania komputera szkodliwym oprogramowaniem. W dniu 29 sierpnia 2019 r. powód padł ofiarą takich działań, gdyż nieznana osoba przy pomocy fałszywej wiadomości „(...)" wysłanej ze skrzynki (...) uzyskała login i hasło do jego bankowości elektronicznej poprzez podszycie się pod serwis internetowy pozwanego banku, z którego to fałszywego serwisu powód wykonał przelew na kwotę 1,36 zł. W tamtym czasie powód kupował kilka akcesoriów samochodowych na portalu (...) i wykonywał kilka przelewów za te zakupy. Uznał, że mógł w którymś przelewie jakiejś kwoty nie dopłacić. Kliknął więc w link prowadzący do systemu płatności i wykonał przelew brakującej kwoty. Według niego, to była strona systemu płatniczego stosowana przy zakupach na (...). Były tam prostokąty z wyborem banku. Powód wybrał z tej strony (...). Podał login i hasło. Nie było żadnego kodu sms przy logowaniu. Następnie wykonał przelew na kwotę 1,36 zł. Autoryzował przelew sms-em. Kolejny raz powód zalogował się 08 września 2019 r. i wtedy zauważył, że ktoś wykonał z jego konta przelewy na łączną kwotę 45.000 zł.

Logowanie do serwisu internetowego pozwanego banku odbywa się poprzez podanie loginu i hasła, dodatkowo wyświetla się obrazek bezpieczeństwa. W przypadku powoda, powód zalogował się poprawnie do serwisu internetowego banku, nie wyświetlił mu się jednak obrazek bezpieczeństwa, a następnie zdefiniował szablon zaufanego odbiorcy i przelał kwotę 1,36 zł - które to czynności wymagały autoryzacji sms-kodem. W pierwszym sms-ie widniała informacja, że jest to autoryzacja nowego odbiorcy, a w drugim sms-ie była podana informacja o autoryzacji kwoty 1,36 zł. Kolejne przelewy, które odbyły się bez wiedzy powoda, były nieautoryzowane, w wyniku wprowadzenia rzeczonego zaufanego odbiorcy. Z punktu widzenia systemu bankowego pozwanego banku nieautoryzowane transakcje na łączną kwotę 45.000 zł zostały zlecone przez powoda.

Na stronach internetowych banku publikowane są informacje o tym, że logując się do serwisów banku, nie należy korzystać z linków nieznanego pochodzenia, umieszczonych w wiadomościach e-mail i sms bądź na stronach www nienależących do banku; że linki te mogą prowadzić na fałszywą stronę banku i służą wyłudzaniu poufnych danych od klientów. Na początku 2019 r. prowadzona była dodatkowo specjalna kampania dotycząca bezpieczeństwa w sieci.

Tego samego dnia, tj. 08 września 2019 r. powód złożył zawiadomienie na policję, jak też reklamację do pozwanego banku.

Zostało wszczęte w tym zakresie postępowanie przygotowawcze prowadzone przez KRP W. pod nadzorem Prokuratury Rejonowej Warszawa-Wola. Dochodzenie pod sygn. (...), zostało najpierw umorzone postanowieniem z dnia 19 marca 2020 r., a następnie Sąd uchylił postanowienie o umorzeniu dochodzenia.

Z kolei reklamacją skierowaną do pozwanego banku powód zażądał zwrotu kwoty 45.000 zł. W odpowiedzi na reklamację powoda bank pismem z dnia 09 września 2019 r. wskazał na brak podstaw do zwrotu żądanej kwoty. Powód złożył odwołanie od tego stanowiska banku pismem z dnia 11 września 2019 r., a pozwany bank pismem z dnia 02 października 2019 r. podtrzymał swoje poprzednie stanowisko. W wyniku tego powód złożył pismo do pozwanego banku w dniu 25 października 2019 r., w którym przedstawił swoje argumenty przemawiające za żądaniem zwrotu dochodzonej kwoty. Powód też w dniu 11 września 2019 r. złożył wniosek o podjęcie interwencji do Rzecznika Finansowego. Rzecznik Finansowy w swoim stanowisku z dnia 03 stycznia 2020 r. skierowanym do pozwanego banku poprosił o ponowne rozpatrzenie sprawy powoda.

Zgodnie z § 14 ust. 3 regulaminu świadczenia usług bankowości elektronicznej, obowiązującym w pozwanym banku, klienta obciążają w pełnej wysokości nieautoryzowane transakcje płatnicze, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia, co najmniej jednego z obowiązków, o których mowa w § 12 ust. 1-3 oraz § 13 ust. 1.

Z kolei zgodnie z § 12 ust. 1-4 oraz § 13 ust. 1 w/w regulaminu:

1. Klient jest zobowiązany do logowania oraz wykonywania dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście z użyciem instrumentów uwierzytelniających.

2. Klient jest zobowiązany do zachowania w tajemnicy informacji zapewniających bezpieczne korzystanie z usług bankowości elektronicznej, w tym informacji przekazanych (...) Bankowi (...) S.A. dla celów weryfikacji oraz nieudostępniania i nieujawniania innym osobom instrumentów uwierzytelniających.

3. Klient jest zobowiązany do należytego zabezpieczenia urządzeń i oprogramowania, o których mowa w § 3 ust. 2, którymi posługuje się w celu korzystania z usług bankowości elektronicznej poprzez stosowanie:

1) wyłącznie legalnego oprogramowania, jego bieżącą aktualizację i instalację poprawek systemowych zgodnie z zaleceniami producentów,

2) aktualnego oprogramowania antywirusowego i antyspamowego oraz zapory firewall,

3) najnowszych wersji przeglądarek internetowych,

4) haseł zabezpieczających przed nieuprawnionym dostępem do komputera osób trzecich.

4. Szczegółowy opis środków, jakie powinien przedsięwziąć Klient w celu zapewnienia bezpieczeństwa dostępu do usług bankowości elektronicznej podawany jest do wiadomości Klientów i Użytkowników na stronie internetowej, oraz w serwisie telefonicznym.

5. Klient jest zobowiązany do niezwłocznego zgłoszenia utraty, kradzieży, przewłaszczenia, nieuprawnionego użycia albo zniszczenia instrumentów uwierzytelniających bądź nieuprawnionego dostępu do usług bankowości elektronicznej:

1) w serwisie telefonicznym pod numerami telefonów, dostępnymi 24 godziny na dobę, podanymi na stronie internetowej,

2) w oddziałach (...) Banku (...) S.A., których aktualny wykaz dostępny jest na stronie internetowej,

3) za pośrednictwem serwisu internetowego.

Powyższy stan faktyczny Sąd Rejonowy ustalił na podstawie wskazanych powyżej dokumentów, które Sąd w całości uznał za wiarygodne, gdyż ich rzetelność i prawdziwość nie była przez strony kwestionowana oraz w oparciu o okoliczności między stronami bezsporne.

Sąd I instancji uznał, że zeznania powoda stanowiły pełnowartościowy dowód w sprawie. Zeznania te były spójne, logiczne, a nadto korelowały z pozostałym zebranym w sprawie materiałem dowodowym. Ani zeznania świadka, ani dowody z dokumentów, nie podważyły wiarygodności zeznań powoda.

Za wiarygodne Sąd Rejonowy uznał zeznania świadka J. G., pracownika pozwanego banku. Sąd wziął pod uwagę ogólną wiedzę świadka o procedurach obowiązujących w banku oraz okoliczności zlecenia nieautoryzowanych przelewów, będące przedmiotem sporu i w tym zakresie Sąd Rejonowy dał wiarę świadkowi w całości.

Zdaniem Sądu Rejonowego powództwo nie mogło podlegać uwzględnieniu.

Na wstępie rozważań Sąd Rejonowy powołał się na art. 6 k.c. i art. 232 k.p.c. zgodnie z którymi na powodzie ciąży obowiązek wykazania roszczenia - zarówno co do zasady jak i wysokości. W ocenie Sądu I instancji powód nie wywiązał się z tego obowiązku.

Zgodnie z art. 46 ust 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych 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 ustawy. Podobny zapis znalazł się w § 14 ust. 3 regulaminu świadczenia usług bankowości elektronicznej pozwanego banku.

Sąd I instancji przywołał wyrok z dnia 24 maja 2018 r. Sądu Apelacyjnego w Warszawie w sprawie sygn. akt VI ACa 217/17 w którym to wyroku Sąd wskazał, że „jeśli transakcje zostały zrealizowane bez zgody płatnika oraz w okolicznościach, za które nie ponosi on odpowiedzialności, a następnie płatnik dokonał zgłoszenia wystąpienia nieautoryzowanych transakcji, to na dostawcy ciąży obowiązek zwrotu kwot nieautoryzowanych transakcji. Jeśli jednak do nieautoryzowanych transakcji płatnik doprowadził umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia swoich obowiązków (o których mowa w art. 42 ustawy z 2011 r. o usługach płatniczych), wówczas to on, a nie dostawca odpowiada za nieautoryzowane transakcje". W podobnym tonie wypowiedział się Sąd Okręgowy w Warszawie w sprawie o sygn. akt V Ca 1275/19 w wyroku z dnia 11 grudnia 2020 r.

W oparciu o zebrany w sprawie materiał dowodowy Sąd Rejonowy ustalił, że sam powód doprowadził do tego, że przestępcy znaleźli dostęp zarówno do loginu jak i hasła, jak i sms-kodów i to umożliwiło im wyprowadzenie pieniędzy z kont powoda - rachunku rozliczeniowo-oszczędnościowego o nr (...) i rachunku oszczędnościowego o nr (...).

W ocenie Sądu I instancji okoliczność ta bezspornie wskazywała, że to powód dopuścił się rażącego niedbalstwa.

Zdaniem sądu Rejonowego istotnym było ustalenie, czy w niniejszej sprawie niedbalstwo po stronie powodowej miało cechy rażącego niedbalstwa, jako kwalifikowanej formy winy czy cechy „zwykłego" niedbalstwa, o czym decydowało ustalenie wzorca staranności, wymaganego w stosunkach danego rodzaju.

Zgodnie z treścią art. 355 § 1 k.c. „dłużnik obowiązany jest do staranności ogólnie

wymaganej w stosunkach danego rodzaju (należyta staranność)."

Sąd Rejonowy wskazał, iż co do zasady przez należytą staranność należy rozumieć staranność ogólnie wymaganą w stosunkach danego rodzaju. Jej wzorzec ma charakter obiektywny, a z kolei jego zastosowanie w praktyce polega najpierw na dokonaniu wyboru modelu ustalającego optymalny w danych warunkach sposób postępowania,

odpowiednio skonkretyzowanego i aprobowanego społecznie, a następnie na porównaniu zachowania się dłużnika z takim wzorcem postępowania. O tym, czy na tle konkretnych okoliczności można osobie zobowiązanej postawić zarzut braku należytej staranności w dopełnianiu obowiązków, decyduje nie tylko niezgodność jej postępowania z modelem, lecz także uwarunkowana doświadczeniem życiowym możliwość i powinność przewidywania odpowiednich następstw zachowania. Miernik postępowania dłużnika, którego istotą jest zaniechanie dołożenia staranności, nie może być formułowany na poziomie obowiązków niedających się wyegzekwować, oderwanych od doświadczeń, reguł zawodowych, konkretnych okoliczności czy typu stosunków (zob. wyroki SN z dnia 17 maja 2002 r., I CKN 1180/99; z dnia 23 października 2003 r., V CK 311/02; z dnia 08 lipca 1998 r., III CKN 574/97).

Pojęcie należytej staranności jest miernikiem ustalenia winy w postaci niedbalstwa, gdy stanowi ona przesłankę zastosowania określonego przepisu (wyrok Sądu Najwyższego z dnia 30 marca 2000 r. sygn. akt III CKN 709/98).

O stopniu niedbalstwa świadczy stopień staranności, jakiego w danych okolicznościach można wymagać od sprawcy. Niezachowanie podstawowych, elementarnych zasad ostrożności, które są oczywiste dla większości rozsądnie myślących ludzi, stanowi o niedbalstwie rażącym. Poziom elementarności i oczywistości wyznaczają okoliczności konkretnego stanu faktycznego, związane m.in. z osobą sprawcy, ale przede wszystkim zdarzenia obiektywne, w wyniku których powstała szkoda (wyrok Sądu Najwyższego z dnia 10 sierpnia 2007r., sygn. akt II CSK 170/07, por. też wyrok Sądu Najwyższego z dnia 10 marca 2004r., sygn. akt IY CK 151/03).

Sąd Rejonowy zwrócił uwagę, iż artykuł 355 k.c. kładzie wyraźny akcent na rodzaj stosunków, przez co należy rozumieć rodzaj przedsięwziętej aktywności, przy czym uwzględniając rodzaj działalności, należy zważyć, że chodzi o miarę staranności powszechnie przyjętą, do pewnego stopnia obiektywną, wynikającą z nakazów sztuki, umiejętności lub techniki, którą można w konkretnym przypadku ustalić, stosując uchwytne mierniki staranności. Ocena stopnia staranności nie może być dowolna, musi poddawać się weryfikacji (wyrok sądu Najwyższego z dnia 21 września 2007 r., sygn. akt V CSK 178/07).

Sąd I instancji podzielił w pełni stanowisko strony pozwanej co do okoliczności, że to po stronie powodowej doszło do rażącego niedbalstwa, które musiało skutkować oddaleniem powództwa w niniejszej sprawie, bowiem strona pozwana nie zawiniła w żaden sposób tego rodzaju działaniom.

W ocenie Sądu Rejonowego rażące niedbalstwo powoda polegało na braku zachowania wymaganej staranności obejmującej obowiązek i konieczność przestrzegania i respektowania ostrzeżeń dostawcy usługi. Zarówno w chwili zdarzenia, jak i przed oraz po zdarzeniu, na stronie pozwanego banku widniały ostrzeżenia dotyczące zagrożeń w sieci. Jak wynikało z zebranego w sprawie materiału dowodowego - od początku 2019 r. na stronach internetowych pozwanego banku widniała informacja o zagrożeniach w sieci; była to specjalna kampania dotycząca bezpieczeństwa w bankowości internetowej. Dodatkowo bank wprowadził tzw. „obrazek bezpieczeństwa" konieczny do logowania na stronie banku. Powód logując się po uzyskaniu maila wzywającego go do zapłaty kwoty 1,36 zł nie zwrócił uwagi, że na fałszywej stronie banku nie było obrazka bezpieczeństwa, a powinno to wzbudzić jego podejrzenia. Obrazek bezpieczeństwa praktycznie nie jest możliwy do użycia przez oszustów, którzy na fałszywych stronach ograniczają dostęp do aplikacji do loginu i hasła.

Istotnym więc zdaniem Sądu Rejonowego w niniejszej sprawie był fakt, że powód zignorował ostrzeżenia pozwanego, które stale i nieprzerwanie widniały na jego stronie od początku 2019 r. i ta okoliczność świadczyła o rażącym niedbalstwie po stronie powodowej. Wobec potwierdzenia przez powoda dwoma sms-kodami zaufanego odbiorcy, wbrew ostrzeżeniom widniejącym na stronie internetowej pozwanego, kolejne przelewy były nieautoryzowane i spowodowały wyprowadzenie z kont powoda 45.000 zł. Uznać więc należało za zawinione naruszenie elementarnych zasad bezpiecznego korzystania z bankowości elektronicznej, co skutkowało przypisaniem przez Sąd Rejonowy stronie powodowej rażącego niedbalstwa.

Reasumując, gdyby więc powód dochował należytej staranności i czujności przy posługiwaniu się systemem bankowości elektronicznej, nie udostępniłby przestępcom wszystkich danych potrzebnych do dokonania przelewów.

Przy tym w ocenie Sądu Rejonowego, nie doszło do złamania zabezpieczeń systemu bankowego, bowiem sam powód ujawnił osobom nieuprawnionym swoje poufne dane, a więc login, hasło, sms-kod - na fałszywej stronie, umożliwiając w ten sposób sprawcom przestępstwa ich przejęcie, a następnie wykorzystanie bez jego wiedzy. W tym zakresie pozwany zastosował z należytą starannością zabezpieczenia, przyjęte w stosunkach tego rodzaju, a wyłudzenie danych nie wynikało z niesprawności systemów bankowych, czy nieszczelności stosowanych przez bank zabezpieczeń bądź niedochowania należytej staranności w sprawowaniu pieczy nad powierzonymi mu środkami finansowymi klientów, lecz ze sprawności działania oszustów, którzy korzystając z ludzkiej nieświadomości, naiwności, niedbalstwa i pośpiechu, a także innych czynników osłabiających czujność klienta dokonywali tego rodzaju przestępstw, przy korzystaniu przez takie osoby z usług bankowości elektronicznej.

Sąd Rejonowy w oparciu o zgromadzony w sprawie materiał dowodowy ustalił, że to powód dopuścił się rażącego niedbalstwa w wyniku nie zachowania podstawowych zasad bezpieczeństwa, a sprawność i kreatywność sprawców przestępstwa doprowadziła do włamania się na jego konto i ściągnięcia stamtąd znajdujących się tam środków finansowych.

Wobec ustalenia przez Sąd Rejonowy, że to rażące niedbalstwo miało miejsce po stronie powodowej, zdaniem Sądu nie sposób było przypisać pozwanemu niewłaściwego wykonania umowy rachunku bankowego.

Z tych względów, działając na podstawie wyżej cytowanych przepisów, Sąd I instancji oddalił powództwo.

O kosztach procesu Sąd Rejonowy orzekł jak w punkcie II. wyroku na podstawie art. 98 § 1 i § 3 k.p.c. nakładając na powoda, jako stronę przegrywającą postępowanie, obowiązek zwrotu wszystkich kosztów.

Apelację od powyższego wyroku wniósł powód, zaskarżając go w całości, zarzucając mu:

1. prawa materialnego, tj.:

a) art. 46 ust. 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych poprzez jego błędną wykładnię i przyjęcie, że pokrzywdzony, który pada ofiarą przestępstwa phishingu dopuszcza się rażącego niedbalstwa, gdyż nie dochowuje należytej staranności i czujności przy posługiwaniu się systemem bankowości elektronicznej, podczas gdy zgodnie z ugruntowaną linią orzeczniczą ofiarom phishing nie można przypisać rażącego niedbalstwa,

b) art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych poprzez jego niezastosowanie i uwolnienie Pozwanego od odpowiedzialności za dokonanie kwestionowanych w niniejszym postępowaniu nieautoryzowanych transakcji, przy jednoczesnym obarczeniu odpowiedzialnością Powoda,

c) art. 471 k.c. poprzez jego niezastosowanie na skutek błędnego przyjęcia, że nie zachodzą przesłanki odpowiedzialności kontraktowej po stronie Pozwanego,

2. prawa procesowego tj.:

a) art. $235^{(1)}$ § 2 k.p.c. poprzez pominięcie dowodu z opinii Rzecznika Finansowego i nie wydanie postanowienia dotyczącego pominięcia tego dowodu wraz ze wskazaniem podstawy prawnej tego rozstrzygnięcia, co skutkowało nieuwzględnieniem przez Sąd I instancji stanowiska Rzecznika Finansowego, zgodnie z którym ofiara phishingu nie dopuszcza się rażącego niedbalstwa,

b) art. 233 § 1 k.p.c. poprzez błędną ocenę zgromadzonego w sprawie materiału dowodowego z naruszeniem zasad doświadczenia życiowego oraz logicznego rozumowania, polegającą w szczególności na błędnym przyjęciu, że system autoryzacji klienta i transakcji u Pozwanego był standardowy i odpowiadał systemom w innych bankach, a strona pozwana nie zawiniła w żaden sposób w przedmiotowej sprawie,

Wobec powyższego apelujący wniósł o:

1. zmianę zaskarżonego wyroku w całości i orzeczenie odmiennie co do istoty sprawy poprzez zasądzenie na rzecz Powoda od Pozwanego kwoty 45.000,00 zł wraz z odsetkami ustawowymi za opóźnienie liczonymi od dnia 10 września 2019 r. do dnia zapłaty, a także zasądzenie na rzecz Powoda od Pozwanego kosztów postępowania w I instancji, w tym kosztów zastępstwa procesowego według norm przepisanych, wraz z odsetkami ustawowymi za opóźnienie zgodnie z art. 98 § 1^1 k.p.c.,

2. zasądzenie od strony pozwanej na rzecz Powoda kosztów postępowania apelacyjnego, w tym kosztów zastępstwa adwokackiego według norm prawem przepisanych wraz z odsetkami ustawowymi za opóźnienie zgodnie z art. 98 § 1^1 k.p.c.

Strona pozwana wniosła o oddalenie apelacji oraz o zasądzenie od powoda na rzecz pozwanego zwrotu kosztów zastępstwa procesowego za druga instancję, według norm przepisanych.

Sąd Okręgowy zważył, co następuje:

Apelacja zasługiwała na uwzględnienie.

Sąd Okręgowy co do zasady podziela i przyjmuje za własny ustalony przez Sąd Rejonowy stan faktyczny. Ustalenia poczynione przez Sąd Rejonowy, jako znajdujące oparcie w zgromadzonym w sprawie materiale dowodowym uznać należało za prawidłowe. Nie sposób jednak zgodzić się ze stanowiskiem Sądu Rejonowego o przyjęciu rażącego niedbalstwa po stronie powoda, jako przyczyny zwalniającej pozwany bank z odpowiedzialności. W ocenie Sądu Okręgowego nie są oczywiste okoliczności, że od początku 2019 r. stale i nieprzerwanie widniały na stronie internetowej pozwanego ostrzeżenia dotyczące zachowania należytego bezpieczeństwa podczas logowania do bankowości mobilnej banku. Oczywiście rynek usług bankowości elektronicznej stale się rozwija i świadomość jego klientów na dzień dzisiejszy z pewnością jest większa, jednak Sąd Okręgowy nie podziela przekonania Sądu Rejonowego, że w 2019 r. metody działania hakerów i środki obrony przed nimi były powszechnie znane.

W ocenie Sądu Okręgowego, zarzuty apelującego zasługiwały na uwzględnienie. W szczególności zasadnie skarżący zarzuca naruszenie przepisów ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2017. 2003 t.j.). Wskazana ustawa stanowi akt prawny, który w sposób kompleksowy reguluje rynek usług płatniczych-określa zarówno zasady podejmowania i prowadzenia działalności na rynku usług płatniczych przez dostawców wskazanych w art. 4 ust. 2, jak i prawa i obowiązki dostawców usług płatniczych związane ze świadczeniem usług płatniczych (por. Barbara Bajor, Jan Brylski, Anna Zalcewicz, Ustawa o usługach płatniczych. Komentarz, wyd. II. LEX 2017).

Stosownie do postanowień art. 1 ustawa określa zasady świadczenia usług płatniczych oraz wydawania i wykupu pieniądza elektronicznego. Zwrócić należy uwagę, że ustawa w swojej treści zawiera rozwiązania prawne zarówno natury prywatnoprawnej, jak i publicznoprawnej. W ustawie określone zostały warunki świadczenia usług płatniczych, w szczególności wymogi dotyczące obowiązków informacyjnych dostawców usług płatniczych w przypadku zawierania umów ramowych oraz w odniesieniu do każdej pojedynczej usługi płatniczej. Uregulowane zostały również zasady, których zasadniczym celem jest zwiększenie przejrzystości postanowień umów o świadczenie usług płatniczych i w sposób jasny oraz zrozumiały określenie praw i obowiązków stron umowy, w tym w szczególności rodzajów i wysokości pobieranych opłat z tytułu świadczonej usługi. W ten sposób został podkreślony prokonsumencki charakter rozwiązań ustawy.

W art. 2 ww. ustawy zamieszczono tzw. słownik zawierający objaśnienia określeń ustawowych, co pozwala na identyfikację stron stosunku prawnego - powoda jako płatnika oraz strony pozwanej jako dostawcę usługi. Przez usługi płatnicze ustawa rozumie działalność polegającą między innymi na wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub innego dostawcy przez wykonywanie usług polecenia przelewu. Działalność w zakresie świadczenia usług płatniczych może być wykonywana wyłącznie przez dostawców usług płatniczych, którymi mogą być podmioty wymienione w ustawie, m.in. bank krajowy w rozumieniu art. 4 ust. 1 pkt 1 ustawy Prawo bankowe.

Rozdział 2 działu III ustawy poświęcony został problematyce autoryzacji transakcji płatniczych, skutków braku autoryzacji transakcji oraz zasad i zakresu odpowiedzialności dostawcy i płatnika za transakcje nieautoryzowane, jak też nienależycie wykonane czy niewykonane. Autoryzacja transakcji oznacza wyrażenie zgody na dokonanie transakcji płatniczej, czyli stanowi oświadczenie woli użytkownika składane z zamiarem i świadomością wywołania określonych skutków prawnych, tj. dokonania transakcji płatniczej. Sposób wyrażenia zgody (czyli sposób autoryzacji transakcji) jest uzależniony od rodzaju transakcji płatniczej, wykorzystywanego instrumentu płatniczego czy sposobu zlecania usługi płatniczej (w formie papierowej czy drogą elektroniczną). Sposób autoryzowania transakcji określony jest w załączonych do umowy ramowej regulaminach wskazujących, w jaki sposób dochodzi do autoryzacji transakcji (np. przez użycie kolejnego kodu z karty kodów). Prawidłowa, zgodna z określonymi w załączonych do umowy ramowej regulaminami, autoryzacja jest zasadniczym elementem w procesie przeprowadzania transakcji. Przede wszystkim od ustalenia, czy doszło do autoryzacji transakcji płatniczej przez użytkownika, czy też mamy do czynienia z transakcją nieautoryzowaną, zależy odpowiedzialność zarówno dostawcy, jak i płatnika za transakcję płatniczą. Natomiast od ustalenia, z jakich przyczyn doszło do wykonania nieautoryzowanej przez płatnika transakcji, zależy zakres odpowiedzialności dostawcy i obowiązku zwrotu kwot nieautoryzowanych transakcji.

W przypadku wystąpienia nieautoryzowanych przez płatnika transakcji płatniczych konieczne jest ustalenie, w jakich okolicznościach doszło do nieautoryzowanych transakcji: czy z winy płatnika wskutek naruszenia podstawowych obowiązków płatnika określonych w art. 42 u.u.p., czy też z powodu okoliczności, za które nie ponosi on odpowiedzialności, czy jednak z powodu okoliczności, za które ponosi odpowiedzialność dostawca. Od powyższych ustaleń uzależniona jest możliwość uzyskania przez płatnika zwrotu kwot nieautoryzowanych przez niego transakcji.

Przyjęte rozwiązanie sugeruje, że płatnik, zlecając wykonanie transakcji płatniczej, czyli składając oświadczenie woli, musi autoryzować transakcję. Oznacza to, że samo złożenie oświadczenia woli, na mocy którego płatnik zleca wykonanie transakcji, nie jest wystarczające - nie jest równoznaczne z wyrażeniem zgody.

W art. 42 ustawy wskazane zostały obowiązki użytkownika, które mają na celu zapewnienie minimum bezpieczeństwa transakcji płatniczych realizowanych z wykorzystaniem instrumentu płatniczego. Podstawowym obowiązkiem użytkownika jest więc korzystanie z instrumentu płatniczego zgodnie z postanowieniami umowy ramowej (jak również zgodnie z dołączonymi do umowy ramowej regulaminami, które stanowią integralną część umowy i określają zasady korzystania z instrumentu płatniczego - ust. 1 pkt 1). Kolejny obowiązek użytkownika - zgodnie z treścią ust. 1 pkt 2 - polega na powiadomieniu w przypadku utraty, kradzieży, przywłaszczenia czy też stwierdzenia, że doszło do nieuprawnionego skorzystania z instrumentu, dostawcy (lub podmiotu wskazanego w tym celu przez dostawcę) o zaistnieniu powyższego zdarzenia.

Artykuł 45 ustawy zawiera szczególną regułę dotyczącą ciężaru dowodu w przypadku dochodzenia roszczeń z tytułu nieautoryzowanych, nienależycie wykonanych lub niewykonanych transakcji. W przypadku powyższych roszczeń ciężar udowodnienia, że transakcja została autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Przypomnieć należy, że zgodnie z art. 6 k.c. ciężar udowodnienia faktu spoczywa na osobie, która z tego faktu chce wywodzić skutki prawne dla siebie. Oznaczałoby to, że jeśli użytkownik kwestionuje fakt autoryzowania transakcji przez siebie, musiałby to wykazać. Rozwiązania przyjęte w omawianej ustawie przerzucają ciężar udowodnienia na dostawcę. Stanowią one wyraz prokonsumenckiego charakteru ustawy. Ciężar udowodnienia, że transakcja była autoryzowana przez użytkownika, ciąży na dostawcy, czyli na profesjonaliście, nawet jeśli to użytkownik występuje z roszczeniem, twierdząc, że nie on autoryzował transakcji. Fakt zarejestrowanego użycia instrumentu płatniczego, czyli - należy przyjąć - użycia instrumentu płatniczego zgodnie z procedurami i przy zastosowaniu ustalonych sposobów autoryzacji, nie oznacza, że transakcja została autoryzowana przez użytkownika. W przypadku zgłoszenia przez użytkownika transakcji, które obciążają jego rachunek płatniczy i które były prawidłowo autoryzowane, czyli zlecone i zrealizowane zgodnie z przewidzianą procedurą, a które użytkownik wskazuje jako przez niego nieautoryzowane, dostawca musi udowodnić fakt autoryzacji transakcji przez użytkownika. Jednak dostawca musi przywołać inne dowody niż sam fakt prawidłowego skorzystania z procedur autoryzacji przewidzianych umową. Dostawca może przytoczyć dowody wykazujące, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji (np.

przekazał kartę i PIN członkowi rodziny) albo wskutek rażącego niedbalstwa naruszył jeden z obowiązków określonych w art. 42 u.u.p., czyli nie przechowywał informacji w sposób zapewniający bezpieczeństwo.

Zasady odpowiedzialności dostawcy oraz płatnika w przypadku wystąpienia nieautoryzowanych transakcji ustawodawca ustala w art. 46 ustawy. W świetle ust. 1 w przypadku wystąpienia nieautoryzowanych transakcji dostawca jest zobowiązany do zwrotu płatnikowi kwoty nieautoryzowanej transakcji niezwłocznie. Podstawowa zasada wskazuje więc obowiązek zwrotu przez dostawcę kwot nieautoryzowanych transakcji. Jeśli jednak do nieautoryzowanych transakcji płatnik doprowadził umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia swoich obowiązków (o których mowa w art. 42 u.u.p.), wówczas odpowiada za wszystkie nieautoryzowane transakcje. O winie płatnika można mówić wówczas, gdy zaistniałe zdarzenie (czyli wystąpienie nieautoryzowanych transakcji) nastąpiło wskutek okoliczności, za które ponosi on odpowiedzialność.

Zobowiązanie banku jako profesjonalnego podmiotu jest determinowane poprzez ustawowe obowiązki wskazane m.in. w art. 43 ust. 1 ustawy o usługach płatniczych. Pozwany bank nie wywiązał się z ich wypełnienia w stosunku do powoda. W szczególności nie zapewnił, by indywidualne zabezpieczenia instrumentu płatniczego nie były dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu. Gdyby bowiem zabezpieczenia transakcji elektronicznych stosowane przez pozwanego były właściwe, nie doszłoby do dokonania na rachunku powoda transakcji przez nieuprawnione do tego osoby.

Trafne są zarzuty apelacji, że powód jako klient banku nie naruszył obowiązków, o których mowa w art. 46 ust. 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych umyślnie lub wskutek rażącego niedbalstwa. Z pewnością działanie powoda nie było umyślne, skoro tuż po dokonaniu zakupu części samochodowych na portalu (...) otrzymał wiadomość „(...)" wysłaną ze skrzynki (...) sugerującą mu iż zalega on z kwotą 1,36 zł względem sprzedawcy z tego portalu. Zdaniem Sądu Okręgowego powodowi nie można również przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa. Komputer powoda posiadał zainstalowane oprogramowanie antywirusowe. Powód nie udostępniał świadomie identyfikatora, hasła ani innych danych jakimkolwiek osobom trzecim. W dniu 29 sierpnia 2019 r. powód wykonywał pewne czynności w systemie bankowości internetowej, jednak dokonanie przelewów na łączną kwotę 45.000 zł z rachunków bankowych powoda nastąpiło poza jego wiedzą i bez autoryzacji przez powoda. Oszust w wiadomości „(...)" wysłanej ze skrzynki (...) uzyskał login i hasło do jego bankowości elektronicznej poprzez podszycie się pod serwis internetowy pozwanego banku, z którego to fałszywego serwisu powód wykonał przelew na kwotę 1,36 zł. Doszło wprawdzie do potwierdzenia transakcji za pomocą właściwego narzędzia, jednak wykonanie kolejnych przelewów nastąpiło bez wyrażenia zgody przez powoda na ich dokonanie. Powód zdefiniował szablon zaufanego odbiorcy i przelał kwotę 1,36 zł - które to czynności wymagały autoryzacji sms-kodem. W pierwszym sms-ie widniała informacja, że jest to autoryzacja nowego odbiorcy, a w drugim sms-ie była podana informacja o autoryzacji kwoty 1,36 zł. Kolejne przelewy, które odbyły się bez wiedzy powoda, były nieautoryzowane, w wyniku wprowadzenia rzeczonego zaufanego odbiorcy. Jest niewątpliwie uchybieniem po stronie powoda, że niezbyt precyzyjnie weryfikował komunikaty na ekranie komputera, w pewnym zakresie z pewnością działaniu powoda można postawić zarzut nienależytej staranności, jednakże nie w stopniu rażącym. Z drugiej jednak strony trzeba wziąć pod uwagę profesjonalizm przestępstwa - sprawca nie został wykryty. Jednocześnie wiedza odnośnie różnic w wyglądzie strony banku i strony fałszywej jest wiedzą, którą dysponuje profesjonalista, ale nie jest powszechnie dostępna zwykłemu użytkownikowi, który zazwyczaj nie zwraca uwagi na istotne detale. Uchybienia powoda, które zaistniały nie mogą być kwalifikowane jako rażące niedbalstwo. Tym bardziej, iż podnoszona przez stronę pozwaną kwestia braku możliwości odtworzenia przez przestępców obrazka identyfikującego nie została wykazana w stopniu wystarczającym.

Sąd Okręgowy pragnie także zwrócić uwagę na te aspekty działania pozwanego, które budziły zastrzeżenia co do jego profesjonalizmu. Stosownie do art. 50 ust. 2 ustawy prawo bankowe na bankach ciąży powinność dołożenia szczególnej staranności w zakresie prowadzenia rachunków bankowych oraz zapewnienia maksimum bezpieczeństwa dla wkładów pieniężnych i przeciwdziałania wypłaty tych środków na rzecz osób nieuprawnionych. Trudno było uznać jako w pełni odpowiadające tym wymogom działanie polegające na braku odpowiedniej reakcji na dokonywane

na kontach powoda operacje bankowe dotyczące przelewu w krótkim czasie znacznych kwot, odpowiadających praktycznie całości wkładów.

Z powyższych względów Sąd Okręgowy zmienił zaskarżone orzeczenie zgodnie z art. 386 § 1 k.p.c., zasądzając na rzecz powoda od strony pozwanej kwotę 45.000 zł wraz z ustawowymi odsetkami za opóźnienie od dnia 10 września 2019 r. do dnia zapłaty oraz kwotę 4.634 zł (zwrot kosztów zastępstwa procesowego, opłaty od pozwu oraz opłaty skarbowej od udzielonego pełnomocnictwa) tytułem zwrotu kosztów procesu.

O kosztach procesu za instancję odwoławczą orzeczono zgodnie z zasadą wyrażoną w art. 98 § 1 i 3 k.p.c. zasądzając od pozwanego na rzecz powoda kwotę 2.800 zł. (1000 zł tytułem zwrotu opłaty od apelacji oraz 1800 zł tytułem zwrotu kosztów zastępstwa procesowego w instancji odwoławczej).