Sygn. akt: I C 439/22

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 13 grudnia 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 6 grudnia 2022 r. w G.

sprawy ***z powództwa J. S.***

przeciwko (...) S.A. z siedzibą w W.

o zapłatę

I. zasądza od pozwanego na rzecz powoda kwotę 30186, 71 zł (trzydzieści tysięcy sto osiemdziesiąt sześć złotych i siedemdziesiąt jeden groszy) wraz z odsetkami ustawowymi za opóźnienie od 22 sierpnia 2020 r. do dnia zapłaty,

II. zasądza od pozwanego na rzecz powoda kwotę 5127 zł (pięć tysięcy sto dwadzieścia siedem złotych) z tytułu zwrotu kosztów postępowania.

UZASADNIENIE

Powód J. S. wniósł pozew przeciwko (...) S.A. z siedzibą w W. o zapłatę kwoty 30.186,71 zł wraz z odsetkami ustawowymi za opóźnienie od dnia 22 sierpnia 2020r. do dnia zapłaty.

W uzasadnieniu pozwu powód podniósł, że w ramach umowy zawartej z (...) Bankiem S.A. z siedzibą w W. korzystał z usług bankowości elektronicznej. W dniu 22 lipca 2020r. usiłując dokonać płatności kartą kredytową powód zorientował się, że na karcie nie ma środków i stwierdził w historii transakcje z dnia 13 lipca 2020r., których nie zlecał, na łączną kwotę 30.186,71 zł. Wszystkie zostały dokonane w jednym dniu, w krótkich odstępach czasu, w dwóch miejscach na terenie Rumunii. Transakcje odbyły się bez wiedzy powoda i nie były przez niego autoryzowane. Powód padł ofiarą tzw. ataku pshisingowego. W dniu kradzieży i w okresie poprzedzającym powód przebywał we Francji. W tym czasie otrzymał informację od firmy kurierskiej (...) o planowanym dostarczeniu zamówionej wcześniej z zagranicy przesyłki i zlecił kurierowi pozostawienie przesyłki w punkcie odbioru. W dniu 13 lipca 2020r. powód otrzymał informację od osoby podszywającej się pod firmę kurierską, że przesyłka nie może zostać doręczona z uwagi na błędny adres. Przez podany w mailu link powód wszedł na stronę wyglądającą jak strona (...), gdzie uzupełnił dane adresowe i wobec informacji, iż przy trzeciej próbie doręczenia pobiera się opłatę w kwocie 12 zł, kliknął na link prowadzący do systemu płatności. Powód złożył reklamację, na którą pozwany udzielił odpowiedzi dopiero w dniu 26 sierpnia 2020r. odrzucając reklamację i pobierając z rachunku karty zwróconą wcześniej kwotę. Zdaniem powoda nie można podzielić stanowiska banku, iż działanie powoda było umyślne, skoro po wcześniejszym kontakcie firmy kurierskiej i przekierowaniu przesyłki otrzymał wiadomość od osoby podszywającej się pod ten podmiot sugerującej konieczność dopłaty 12 zł. Nadto, powodowi nie można przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa, gdyż komputer posiadał zainstalowane oprogramowanie antywirusowe, powód korzystał z legalnego oprogramowania, nie udostępniał świadomie identyfikatora i hasła osobom trzecim. W ocenie powoda to bank – wbrew obowiązkowi wynikającemu z art. 50 Prawa bankowego – stosował niewystarczające

zabezpieczenia przed ww. działaniami przestępczymi i zaniżał standardy bezpieczeństwa powierzonych środków pieniężnych.

(pozew, k. 3-10)

Pozwany wniósł o oddalenie powództwa w całości. Pozwany zwrócił uwagę, że regulamin obsługi klientów w ramach bankowości detalicznej (...) S.A. nakładał na klientów obowiązek chronienia indywidulanych danych uwierzytelniających, niepodawania ich żadnym osobom trzecim lub ich przechowywania z zachowaniem należytej staranności. Podobnie kwestię ochrony danych karty płatniczej określał regulamin kart płatniczych, zobowiązując do nieudostępniania karty ani kodów identyfikujących. Ujawnienie ww. danych przez klienta zgodnie z ww. regulaminami było równoznaczne z niezachowaniem należytej staranności. Powód kliknął w link przesłany przez nieznaną osobę, podał na niezaufanej stronie internetowej co najmniej dane karty (nr karty, kod bezpieczeństwa CVV, datę ważności karty), a także zaakceptował zarejestrowanie karty w aplikacji A. P., co umożliwiło osobom trzecim użycie karty i wykonanie transakcji z jego rachunku. Powód nie zachował zatem należytej staranności, nie zabezpieczając danych dotyczących karty. Działanie powoda naruszało podstawowe obowiązki w zakresie bezpiecznego korzystania z kart płatniczych nałożone przez regulamin i stanowiło przejaw rażącego niedbalstwa. Ponadto, zgodnie z regulaminami na kliencie spoczywał obowiązek zabezpieczenia sprzętu, na którym korzysta z danego sposobu dostępu do banku poprzez instalację i regularne aktualizowanie legalnego oprogramowania, w tym systemów i programów chroniących przed wirusami, internetowymi robakami i spamami. Powód nie przedstawił żadnych dowodów na posiadanie takiego oprogramowania. Regulamin zobowiązywał powoda także do przestrzegania wskazówek bezpieczeństwa zamieszczanych na stronie banku oraz zapoznawania się na bieżąco z komunikatami bezpieczeństwa. Mimo kampanii informacyjnych prowadzanych przez bank powód sam autoryzował operację dodania karty na obcym urządzeniu i w ten sposób wyraził zgodę na dokonywanie transakcji prze osobę trzecią. Tym samym zachodzi przesłanka wyłączająca odpowiedzialność pozwanego przewidziana w art. 46 ust. 3 ustawy o usługach płatniczych. Ponadto, pozwany zwrócił uwagę, że transakcje wykonane z rachunku powoda każdorazowo zatwierdzono zgodnie z podstawowymi metodami potwierdzania transakcji A. P.. W świetle przepisów jest to jednoznaczne ze zgodą na obciążanie rachunku. Taka transakcja ma status wykonania zgodnie z zasadami silnego uwierzytelnienia i ma status ważnej i zawartej, co nie daje podstaw do prowadzenia procesu chargeback. Zlecone operacje nie mogły podlegać jakiejkolwiek dodatkowej weryfikacji przez system banku, nie istnieją bowiem możliwości techniczne, by dyspozycje wydawane jak w niniejszym przypadku, mogły być wychwycone przez system informatyczny banku, jako składane przez osobę nieuprawnioną. Zdaniem pozwanego także wysokość i ilość transakcji nie odbiega znacząco od jego profilu transakcyjności. Powód bowiem wielokrotnie dokonywał płatności kartą za granicą, na kwoty wyższe niż transakcje kwestionowane, w tym wykonywał transakcje bezstykowe za granicą.

(odpowiedź na pozew, k. 59-69)

Sąd ustalił następujący stan faktyczny:

W dniu 5 grudnia 2003r. powód J. S. zawarł z (...) Bankiem S.A. z siedzibą w W. (poprzednikiem prawnym pozwanego (...) S.A. z siedzibą w W.) umowę o korzystanie z karty płatniczej nr (...). Na podstawie przedmiotowej umowy bank wydał powodowi kartę kredytową V., zobowiązał się wobec powoda do rozliczania operacji dokonanych przy użyciu karty, a także umożliwił dysponowanie środkami udostępnionymi przez bank na rachunku do wysokości przyznanego limitu.

(dowód: umowa o korzystanie z karty płatniczej nr (...), k. 13-14)

Do umowy łączącej strony zastosowanie miał Regulamin rachunków dla osób fizycznych i klientów P. B. w ramach bankowości detalicznej (...) S.A., w którym zapisano zasady, na których pozwany bank otwiera i obsługuje rachunki oraz oferuje usługi dodatkowe dla klientów P. B.. W ust. 1 pkt 2) lit c) regulaminu wskazano, że informacje o zasadach wydawania i korzystania z kart debetowych do rachunków zostały określone w regulaminie kart debetowych.

W Regulaminu kart kredytowych dla osób fizycznych i klientów P. B. w ramach bankowości detalicznej (...) SA w rozdziale „Jak bezpiecznie korzystać z karty?" wskazano m.in. sposoby ochrony i przechowywania karty oraz zabezpieczenia danych dotyczące karty, w tym wskazano, że

- chroń kartę i starannie ją przechowuj. Nie umieszczaj karty (np. w formie opaski lub breloka) na innych osobach, zwierzętach lub rzeczach, które mogłyby: a) zmniejszyć/odebrać Ci kontrolę nad kartą, b) powodować naruszenie praw własności przemysłowej związanych z kartą lub innych praw przysługujących nam, organizacji płatniczej lub innym osobom;

- dbaj o to, aby Twoje dyspozycje, w tym płatności, które zlecasz, były prawidłowe i zgodne z Twoją intencją;

- chroń indywidualne dane uwierzytelniające, w tym: a) to informacje poufne, które powinieneś znać jedynie Ty. Nie możesz ich udostępniać innym osobom, firmom czy instytucjom - w tym np. swoim bliskim czy naszym pracownikom, b) jeśli ujawnisz je - uznamy, ze nie zachowałeś należytej staranności;

- nie udostępniaj karty, ani kodów identyfikacyjnych innym osobom. Zadbaj o to, aby nikt nie podejrzał kodu identyfikacyjnego, gdy np. płacisz w sklepie lub wypłacasz gotówkę;

- zapamiętaj (...) i nigdzie go nie zapisuj (ani na kartce, ani w notesie, kalendarzu, komputerze, telefonie czy innym urządzeniu);

- odpowiednio zabezpieczaj sprzęt, na którym korzystasz z danego sposobu dostępu, tj.: a) zachowuj fabryczne zabezpieczenia urządzeń, b) zainstaluj i regularnie aktualizuj legalne oprogramowanie: system oraz programy chroniące przed wirusami, internetowymi robakami i spamem, c) korzystaj z oprogramowania typu firewall, d) pobierz aplikację mobilną z autoryzowanego sklepu: A. Store (dla systemu (...)) lub G. P. (Android), e) nie korzystaj z aplikacji automatyzujących;

- pamiętaj, że nie ponosimy odpowiedzialności za transakcje kortowe i dyspozycje osób trzecich, jeśli nie wypełniłeś obowiązków związanych z bezpiecznym używaniem karty.

Nadto, w ww. Regulaminie wskazano, że: jeśli ujawniłeś innym osobom - w tym członkom rodziny: a) swój identyfikator, lub b) indywidualne dane uwierzytelniające będzie to oznaczało, że nie zachowałeś należytej staranności, o której mowa w ustawie o usługach płatniczych.

Zgodnie z punktem II.1 Regulaminu korzystania z kart płatniczych (...) SA w ramach A. P. A. P. to technologia, która pozwala płacić za pomocą urządzeń mobilnych marki A.. Aby to było możliwe, musisz dodać kartę płatniczą do aplikacji W.. Zgodnie z pkt V ust. 2 i 3 tegoż Regulaminu, aby dodać kartę do aplikacji W. musisz podać szczegółowe dane karty: pełny numer karty, jej datę ważności i kod (...). Gdy dodasz kartę, otrzymasz od nas na zarejestrowany numer telefonu komórkowego, jednorazowy kod weryfikacyjny, którym potwierdzisz dodanie karty w aplikacji W.. Dodanie karty możesz również potwierdzić w naszej aplikacji mobilnej.

(dowód: Regulamin rachunków dla osób fizycznych i klientów P. B. w ramach bankowości detalicznej (...) S.A. k. 75-79, Regulamin usług płatniczych dla osób fizycznych i klientów P. B. w ramach bankowości detalicznej (...) SA k. 80-85, Regulamin korzystania z kart płatniczych (...) SA w ramach A. P., k. 86-90)

Na początku lipca 2020r. powód kupił oponę, która miała zostać dostarczona z Niemiec przez firmę kurierską (...). W dniu wyjazdu na zgrupowanie do Francji powód został poinformowany telefonicznie przez kuriera (...) o planowanym dostarczeniu przesyłki. Powód poprosił kuriera o pozostawienie przesyłki w punkcie odbioru. Po kilku dniach powód otrzymał od osoby podszywającej się pod firmę kurierską (...) e – maila z informacją, że przesyłka została odwieziona do magazynu zbiorczego w G. z uwagi na nieprawidłowy adres doręczenia. W treści e – maila był link prowadzący do strony internetowej. Powód kliknął na link i został przekierowany na stronę, która przypominała stronę firmy kurierskiej (...). W formularzu znajdującym się na tej stronie powód wpisał nowy adres do doręczeń. Na stronie

znajdowała się informacja, że przesyłkę próbowano już dwukrotnie doręczyć, a trzecia próba jest płatna, zaś koszt wynosi 12 zł. Powód kliknął na link, który przekierował go na stronę podobną do strony operatora karty płatniczej. W znajdującym się na tej stronie formularzu powód wpisał numer karty kredytowej, kod CVV, datę ważności karty, swoje imię i nazwisko. Następnie, powód otrzymał z banku na swój numer telefonu zarejestrowany w systemie banku wiadomość sms o treści: „Wprowadź kod ****** aby potwierdzić aktywacje karty w A. P.”. Powód wpisał ten kod w otrzymanym formularzu i wysłał go.

(dowód: przesłuchanie powoda J. S., płyta CD k. 147, zrzut z systemu powiadomień autoryzacji sms, k. 91)

Powód korzystał z urządzenia M. z oryginalnym, legalnym oprogramowaniem antywirusowym, które aktualizuje się automatycznie. Nadto, powód korzystał z programu MacKeeper.

(dowód: przesłuchanie powoda J. S., płyta CD k. 147)

W dniu 13 lipca 2020 roku na terenie Rumunii – przy użyciu karty – zostały wykonane następujące transakcje:

- (...) na kwotę (...) RON tj. 2443,94 zł na zakupy w D. P. 2;

- (...) na kwotę (...),99 RON tj. 3693,85 zł na zakupy w (...) SA;

- (...) na kwotę (...),98 RON tj. 4107,55 zł na zakupy w (...) SA;

- (...) na kwotę (...) RON tj. 3939,13 zł na zakupy w (...) SA;

- (...) na kwotę (...),96 RON tj. 3739,13 zł na zakupy w A. C.;

- (...) na kwotę (...),90 RON tj. 3792,26 zł na zakupy w A. C.;

- (...) na kwotę 756,18 RON tj. 744,85 zł na zakupy w A. Billa G. C.;

- (...) na kwotę (...),93 RON tj. 1103,16 zł na zakupy w A. Billa G. C.;

- (...) na kwotę 516,51 RON tj. 508,77 zł na zakupy w A. Billa G. C.;

- (...) na kwotę 2430,50 RON tj. 2394,11 zł na zakupy w (...) 1190;

- (...) na kwotę (...) RON tj. 1009,66 zł na zakupy w (...) 1931;

- (...) na kwotę (...),50 RON tj. 2710,30 zł na zakupy w (...) 1931.

(dowód: lista operacji, k. 15-16)

Wcześniej, powód nie dokonywał w ciągu jednego dnia transakcji na kwoty przekraczające 30.000 zł. Najwyższe zakupy przy użyciu karty to zakup biletu lotniczego do USA za kwotę 3.500 zł oraz zakup garnituru za kwotę 2.000 zł. Przy zakupie garnituru, z powodem skontaktował się pracownik banku, aby potwierdzić transakcję. Generalnie, przy użyciu karty dokonywał drobnych zakupów w sklepach. Powód korzystał z karty także za granicą, lecz nigdy w Rumunii. Powód już wcześniej korzystał i dokonywał płatności za pośrednictwem aplikacji A. P..

(dowód: przesłuchanie powoda J. S., płyta CD k. 147)

Powód nie zapoznał się z informacjami widniejącymi na stronie internetowej pozwanego banku ani też wcześniej nie znał metody phishingu.

(dowód: przesłuchanie powoda J. S., płyta CD k. 147)

W dniu 22 lipca 2020r. powód złożył reklamację w pozwanym (...) S.A. Pismem z dnia 26 sierpnia 2020r. pozwany poinformował powoda, że kwestionowane transakcje prawidłowo zatwierdzono zgodnie z § 6 Regulaminu korzystania z kart płatniczych (...) SA w ramach A. P.. Nadto, wskazał, że powód korzystał z fałszywego linku do płatności, gdzie podał dane do karty i dlatego doszło do kwestionowanych operacji. Bank powołał się na art. 46 ust. 3 ustawy o usługach płatniczych odmawiając uwzględnienia reklamacji.

Pismem z dnia 21 września 2020r. pełnomocnik powoda wskazał, że wobec niedotrzymania przez bank 30 – dniowego terminu na rozpatrzenie reklamacji, należy uznać ją za rozpatrzoną zgodnie z wolą klienta, a nadto zaprzeczył, by powód wyraził zgodę na wykonanie spornych transakcji płatniczych i by były one przez niego autoryzowane, a także wezwał do zwrotu kwoty 30.186,71 zł w terminie 3 dni od daty otrzymania pisma.

Ponadto, skierował wniosek do Rzecznika (...) w przedmiocie nieuwzględnienia roszczeń w trybie reklamacyjnym. Mimo powyższego, pismem z dnia 30 kwietnia 2021r. pozwany odmówił zwrotu środków, wskazując, że powód udostępnił wrażliwe dane karty oraz poufny kod sms na fałszywej stronie, co doprowadziło do aktywacji karty mobilnej na obcym urządzeniu.

Pismem z dnia 19 sierpnia 2021r. powód – za pośrednictwem zawodowego pełnomocnika – wezwał pozwanego do zapłaty kwoty 30.186,71 zł w terminie 7 dni licząc od daty otrzymania wezwania.

(dowód: pismo pozwanego z dnia 26 sierpnia 2020r., k. 19-20, pismo powoda z dnia 21 września 2020r., k. 21-22, pismo Rzecznika (...) z dnia 31 marca 2021r., k. 25-27, pismo Rzecznika (...) z dnia 12 listopada 2021r., k. 28-36, pismo Rzecznika (...) z dnia 16 stycznia 2022r., k. 37-42, pisma pozwanego z dnia 30 kwietnia 2021r., k. 43-46, wezwanie do zapłaty z dnia 19 sierpnia 2021r., k. 48 wraz z kopią karty księgi nadawczej, k. 49)

Po złożeniu reklamacji, bank zwrócił na rachunek bankowy powoda kwotę 30.186,71 zł, jednak przy rozpatrzeniu reklamacji bank pobrał tę kwotę.

(dowód: przesłuchanie powoda J. S., płyta CD k. 147)

Powód nie złożył zawiadomienia o popełnieniu przestępstwa, będąc w przekonaniu – po rozmowie z konsultantem banku – że pozwany złoży takie zawiadomienie.

(dowód: przesłuchanie powoda J. S., płyta CD k. 147)

Sąd zważył, co następuje:

Powyższy stan faktyczny Sąd ustalił na podstawie dowodów z dokumentów przedłożonych przez strony, a także dowodu z przesłuchania powoda.

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 stron, Regulaminów, korespondencji stron, a także pism kierowanych przez powoda do Rzecznika (...). 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 (lista operacji na rachunku bankowym, zrzut z systemu powiadomień autoryzacji sms), albowiem nie kwestionowano tego, że załączone do akt sprawy wydruki nie stanowią odzwierciedlenia danych zapisanych na nośnikach czy w systemach elektronicznych banku.

Nadto, Sąd dał wiarę zeznaniom powoda odnośnie okoliczności towarzyszących dokonaniu nieautoryzowanych transakcji, środków bezpieczeństwa stosowanych przez niego przy korzystaniu z instrumentów bankowych,

posiadania legalnego oprogramowania antywirusowego, sposobu korzystania z karty płatniczej czy też przebiegu postępowania reklamacyjnego. W ocenie Sądu zeznania powoda były szczere, spontaniczne, wewnętrznie spójne, a także nie pozostawały w sprzeczności z żadnymi dowodami przedstawionymi przez bank w toku niniejszego postępowania. Zeznania te nie budzą także żadnych wątpliwości Sądu w świetle zasad logicznego rozumowania i zasad doświadczenia życiowego.

Natomiast, na podstawie art. 235^2 § 1 pkt 2 k.p.c., Sąd pominął wnioski dowodowe pozwanego banku o zobowiązanie powoda do złożenia dowodu zakupu legalnego oprogramowania systemu operacyjnego oraz oprogramowania antywirusowego zainstalowanego na urządzeniach, z których powód korzystał logując się do systemu transakcyjnego banku i odbierał kody autoryzacyjne, a także do przedstawienia treści wiadomości e – mail otrzymanej od osób trzecich podających się za firmę kurierską (...). Zważyć należy, iż okoliczności dotyczące legalności oprogramowania, jakie powód miał zainstalowane na swoich urządzeniach były irrelewantne dla rozstrzygnięcia sprawy, albowiem niesporne było, że w rozpatrywanym przypadku nie doszło do zainfekowania urządzenia wirusami, lecz powód padł ofiarą tzw. ataku phishingowego polegającego na podszyciu się przez cyberprzestępców pod firmę kurierską i wyłudzeniu danych umożliwiających dokonywanie transakcji za pomocą karty powoda. Z kolei, okoliczności dotyczące treści wiadomości skierowanej do powoda przez oszustów oraz mechanizmu wyłudzenia danych były bezsporne.

Na wstępie należy odnieść się do kwestii reklamacji skierowanej przez powoda do pozwanego banku. Jak wskazywała strona powodowa reklamacja została zgłoszona przez nią w dniu 22 lipca 2020r., natomiast bank odpowiedział na nią dopiero w dniu 26 sierpnia 2020r., a więc po upływie terminu określonego w ustawie z dnia 5 sierpnia 2015r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym (tekst jednolity Dz.U. z 2022 r. poz. 187), co zdaniem powoda jest równoznaczne z uwzględnieniem reklamacji. Zważyć należy, iż zgodnie z treścią art. 6 ustawy z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym odpowiedzi na reklamację, należy udzielić bez zbędnej zwłoki, jednak nie później niż w terminie 30 dni od dnia otrzymania reklamacji. Do zachowania terminu wystarczy wysłanie odpowiedzi przed jego upływem. Natomiast, wedle art. 8 powołanej ustawy w przypadku niedotrzymania terminu określonego w art. 6, a w określonych przypadkach terminu określonego w art. 7, reklamację uważa się za rozpatrzoną zgodnie z wolą klienta. Należy jednak mieć na względzie, że w postępowaniu wszczętym przez klienta przeciwko podmiotowi rynku finansowego o zapłatę kwoty roszczenia zgłoszonej w reklamacji klienta, art. 8 ustawy z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym nie wyłącza możliwości kwestionowania przez podmiot rynku finansowego zasadności dochodzonego roszczenia; na podmiocie tym spoczywa ciężar dowodu, że powodowi nie przysługuje roszczenie lub przysługuje w niższej wysokości (por. uchwała Sądu Najwyższego z dnia 13 czerwca 2018r., III CZP 113/17, L.). Zatem, samo udzielenie odpowiedzi na reklamację z uchybieniem terminu określonego w art. 6 ustawy o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym nie zamykało pozwanemu drogi do kwestionowania roszczenia powoda i miało jedynie wpływ na rozkład ciężaru dowodu.

Przechodząc do rozważań merytorycznych, należy wskazać, iż w niniejszej sprawie powód dochodził od pozwanego zwrotu kwoty 30.186,71 zł ściągniętej w ramach limitu kredytowego wskutek transakcji wykonanych bez zgody powoda, przy użyciu karty. Podstawę prawną powództwa stanowił przepis art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011r. o usługach płatniczych (tekst jednolity Dz.U. z 2022 r. poz. 2360), 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.

W niniejszej sprawie bank odmówił spełnienia świadczenia powoda, wskazując, że postępowanie powoda naruszało podstawowe obowiązki w zakresie bezpiecznego korzystania z kart płatniczych nałożone przez regulamin i stanowiło przejaw rażącego niedbalstwa. W ocenie Sądu nie sposób jednak podzielić argumentacji pozwanego i uznać, że powód umyślnie doprowadził do nieautoryzowanej transakcji płatniczej bądź dopuścił się wskutek rażącego niedbalstwa naruszenia któregokolwiek z obowiązków o których mowa jest w art. 42 ustawy o usługach płatniczych. Zważyć należy, iż zgodnie ze stanowiskiem judykatury rażące niedbalstwo (culpa lata) jest kwalifikowaną postacią winy nieumyślnej. Oznacza zatem wyższy jej stopień niż w przypadku zwykłego niedbalstwa, leżący już bardzo blisko winy umyślnej (culpa lata dolo aequiparatur). Wykładnia pojęcia rażącego niedbalstwa powinna uwzględniać kwalifikowaną postać braku zwykłej staranności w przewidywaniu skutków. Konieczne jest zatem stwierdzenie, że podmiot, któremu taką postać winy chce się przypisać, zaniedbał takiej czynności zachowującej chronione dobro przed zajściem zdarzenia powodującego szkodę, której niedopełnienie byłoby czymś absolutnie oczywistym w świetle doświadczenia życiowego dostępnego każdemu przeciętnemu uczestnikowi obrotu prawnego i w sposób wprost dla każdego przewidywalny mogło doprowadzić do powstania szkody. Rażące niedbalstwo zachodzi bowiem tylko wtedy, gdy stopień naganności postępowania drastycznie odbiega od modelu właściwego w danych warunkach zachowania się dłużnika (por. wyrok Sądu Najwyższego z dnia 22 kwietnia 2004 roku, II CK 142/03, Lex nr 484721, wyrok Sądu Najwyższego z dnia 25 września 2002 roku, I CKN 969/00, LEX nr 55508). Podkreślić należy, że za niedbalstwo rażące może zostać uznane niezachowanie podstawowych, elementarnych zasad ostrożności, które są oczywiste dla większości rozsądnie myślących ludzi (por. wyrok Sądu Najwyższego z dnia 10 sierpnia 2007r., II CSK 170/07, L.).

Podkreślić należy, iż niesporne pomiędzy stronami były okoliczności dokonania nieautoryzowanych transakcji. Jak wynika bowiem z wiarygodnych zeznań powoda podał on dane swojej karty kredytowej na fałszywej stronie internetowej, do której link został mu przesłany za pośrednictwem poczty elektronicznej przez osobę, która podszywała się pod firmę kurierską (...), z której usług podówczas korzystał. Wcześniej bowiem powód zamówił opony z Niemiec, które miały być mu dostarczone za pomocą firmy kurierskiej (...). Nadto, kilka dni przed nadejściem

ww. wiadomości z powodem skontaktował się kurier z informacją o planowanym dostarczeniu przesyłki. Powód poprosił wówczas o pozostawienie przesyłki w punkcie odbioru. Zatem, w okolicznościach rozpatrywanego przypadku, nadejście e-maila zbiegło się w czasie z terminem doręczenia mu faktycznie zamówionej przesyłki przez tę samą firmę kurierską, co wymieniono w treści e – maila. Jednocześnie, z uwagi na wyjazd zagraniczny powód nie miał możliwości skontaktowania się z firmą kurierską celem ewentualnego wyjaśnienia zaistniałej sytuacji. Zwrócić przy tym należy uwagę, że zarówno e – mail jak i strona internetowa, do której odsyłał link zamieszczony w tej wiadomości łudząco przypominały wyglądem stronę kuriera (...). Strona ta miała służyć zmianie adresu, na jaki miała zostać dostarczona przesyłka. Nadto, na stronie pojawiła się informacja, że przesyłkę próbowano już dwukrotnie doręczyć, a koszt doręczenia jej po raz trzeci wynosi 12 zł. Powód kliknął na link, który przekierował go na stronę podobną do strony operatora karty płatniczej. W znajdującym się na niej formularzu powód wpisał numer dane karty kredytowej. Następnie, powód otrzymał z banku na swój numer telefonu zarejestrowany w systemie banku wiadomość SMS treści: „Wprowadź kod ****** aby potwierdzić aktywacje karty nr ... w A. P.". Powód wpisał ten kod w otrzymanym formularzu i wysłał go. Autoryzacja dodania karty do nieznanego urządzenia umożliwiała osobom trzecim wykonywanie dalszych operacji z wykorzystaniem zabezpieczeń właściwych dla tej metody. W ocenie Sądu nie sposób w opisanych powyżej okolicznościach uznać, że powód jako klient banku naruszył obowiązki, o których mowa w art. 46 ust. 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych umyślnie lub wskutek rażącego niedbalstwa. Przede wszystkim działaniu powoda nie można przypisać cech umyślności, skoro dokonał otrzymał ww. wiadomość e – mail po zamówieniu przesyłki za pośrednictwem tej samej firmy kurierskiej, która została wskazana jako autor maila (faktycznie cyberprzestępcy podszyli się pod firmę kurierską celem wyłudzenia danych karty kredytowej powoda). Koincydencja czasowa pomiędzy terminem doręczenia zamówionej przez powoda przesyłki za pośrednictwem firmy kurierskiej (...) a otrzymaniem spornej wiadomości była główną przyczyną skorzystania z linku, a także podania danych karty kredytowej i dodania karty w A. P.. Powyższe mogło wzbudzić u powoda uzasadnione przekonanie, że wystąpiły problemy z doręczeniem przesyłki, którą faktycznie zamówił za granicą za pośrednictwem ww. firmy kurierskiej (...). Powód nie chciał ujawnić danych nieznanej osobie trzeciej. W ocenie Sądu powodowi nie można również przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa. Powód nie udostępniał bowiem świadomie identyfikatora, czy kodu CVV jakimkolwiek osobom trzecim. Dokonanie transakcji na łączną kwotę 30.186,71 zł nastąpiło poza wiedzą powoda i bez autoryzacji przez niego. C. we wcześniej wiadomości e - mail, podszywając się pod firmą kurierską, z której usług powód faktycznie w owym czasie korzystał, uzyskali dane karty. Co prawda, powód dokonał potwierdzenia aktywacji karty za pomocą kodu autoryzacyjnego przysłanego na jego numer telefonu za pośrednictwem smsa, jednak wykonanie kolejnych przelewów nastąpiło już niewątpliwie bez wyrażenia zgody przez powoda na ich dokonanie. Dwanaście następujących po sobie kolejno transakcji wykonanych w dniu 13 lipca 2020r. na terenie Rumunii nastąpiło bez wiedzy powoda i były przez niego nieautoryzowane. Autoryzacja transakcji oznacza bowiem wyrażenie zgody na dokonanie transakcji płatniczej, czyli stanowi oświadczenie woli użytkownika składane z zamiarem i świadomością wywołania określonych skutków prawnych, tj. dokonania transakcji płatniczej (por. wyrok Sądu Okręgowego w Warszawie z dnia 11 sierpnia 2021 r., XXVII Ca 1352/21, L.). Należy przy tym mieć na uwadze, że wiedza odnośnie różnic w wyglądzie strony firmy kurierskiej i strony fałszywej jest wiedzą, którą dysponuje profesjonalista, ale nie jest to powszechnie dostępna zwykłemu użytkownikowi, który zazwyczaj nie zwraca uwagi na detale różniące obie strony. Tym samym uchybienia powoda nie mogą być kwalifikowane jako rażące niedbalstwo. Dalej, należy wskazać, że w 2020 roku metody działania cyberprzestępców i środki obrony przed nimi nie były powszechnie znane, a zatem nie sposób przyjmować, że wiedza odnośnie zachowania ostrożności przy korzystaniu z płatności internetowych była podstawową, elementarną wiedzą znaną każdemu rozsądnemu użytkownikowi. Nawet, gdyby szczegółowo powód zapoznał się z ostrzeżeniami znajdującymi się na stronie internetowej banku, to w okolicznościach niniejszego przypadku, powód mógł zakładać, że dokonuje zmiany danych adresowych w celu doręczenia mu przesyłki. Podkreślić należy, iż podania analogicznych danych żąda się w wielu sytuacjach jak np. w przypadku rezerwacji pokoju hotelowego za pomocą portalu rezerwacyjnego czy zakupu biletu lotniczego. Dokonanie opłaty za doręczenie przesyłki kurierskiej na rzecz dużego podmiotu cieszącego się renomą na rynku mogło być przez przeciętnego klienta postrzegane w podobnych kategoriach. W świetle zebranego materiału dowodowego należało uznać, że powód nie udostępnił świadomie danych osobom trzecim, a dokonanie transakcji nastąpiło poza jej wiedzą i bez autoryzacji przez niego. Pozwany nie złożył żadnego dowodu, który wskazywałby na to, że powód zatwierdził poszczególne dyspozycje przelewów bankowych, bądź dokonał zakupów przy użyciu karty. Potwierdzenia

poszczególnych transakcji bez wątpienia dokonała osoba trzecia, na co wskazuje m.in. waluta transakcji – lej rumuński (RON), miejsce wykonania transakcji – Rumunia. Zgodnie z zeznaniami powoda w dacie wykonania transakcji przebywał on we Francji na zgrupowaniu. Niewątpliwie uchybieniem po stronie powoda było to, że ujawnił dane karty, a następnie autoryzował dodanie karty w aplikacji A. P., co w okolicznościach niniejszego przypadku pozwala jego działaniu postawić zarzut niedochowania należytej staranności, jednakże nie w stopniu rażącym, jak to usiłuje przedstawić strona pozwana. Doszło wprawdzie do autoryzacji dodania karty za pomocą smsa, jednak nie nastąpiło to z nastawieniem wyrażenia zgody na dokonanie kolejnych kwestionowanych transakcji, lecz w innym celu.

Bez znaczenia dla rozstrzygnięcia sprawy były podnoszone przez pozwanego kwestie dotyczące rodzaju oprogramowania zainstalowanego na urządzeniach powoda, gdyż do wyłudzenia danych doszło w wyniku tzw. phisihingu, a nie zainfekowania urządzenia złośliwym oprogramowaniem, czy wirusami. Tym samym rozważanie powyższych kwestii było bezprzedmiotowe.

Zwrócić należy uwagę, że zgodnie z art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. z 2022 r. poz. 2324) 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 za profesjonalne działanie banku polegające na braku odpowiedniej reakcji na dokonywane kilkunastu transakcji przy użyciu karty w krótkich odstępach czasu opiewające łącznie na znaczną kwotę i przeprowadzone w walucie obcej (lej rumuński) stanowiące płatność za zakupy dokonane na terenie obcego państwa. Zważywszy na profesjonalny charakter działalności pozwanego i posiadaną przez niego wiedzę odnośnie metod wyłudzania środków pieniężnych i phishingu powinien w taki sposób skonfigurować systemy bezpieczeństwa, aby umożliwiały wykrycie tego typu transakcji i ich zablokowanie. Wbrew twierdzeniom pozwanego zawartym w odpowiedzi na pozew w niniejszym przypadku transakcje na rachunku powoda odbiegały od dotychczasowej praktyki właściciela rachunku i posiadacza karty zarówno w zakresie zaciągnięcia zobowiązania kredytowego w znacznej wysokości, jak też – co dla rozstrzygnięcia niniejszej sprawy najistotniejsze – w zakresie wydatkowania środków odpowiadających właściwie całości limitu kredytowego. Okolicznością, która powinna wzbudzić reakcję banku były przede wszystkim wysokość transakcji płatniczych i waluta transakcji. Jak wynika z wiarygodnych zeznań powoda przed 13 lipca 2020r. nie dokonywał on w ciągu jednego dnia transakcji na kwoty przekraczające kwotę 30.000 zł. Najwyższe zakupy dokonane przez niego przy użyciu karty to zakup biletu lotniczego do USA za kwotę 3.500 zł oraz zakup garnituru za kwotę 2.000 zł. Nigdy natomiast nie wykonał przelewów na kwoty dziesięciokrotnie wyższe. Zdaniem Sądu, zważywszy na fakt, iż transakcje odbiegały od dotychczasowej praktyki powoda, bank winien był odpowiednio zareagować np. żądać dodatkowej autoryzacji poszczególnych transakcji bądź też stworzyć odpowiednie algorytmy, które uniemożliwiałyby, bądź ograniczyły tego typu proceder. Zobowiązanie banku jako profesjonalnego podmiotu jest determinowane poprzez ustawowe obowiązki wskazane m.in. w art. 43 ust. 1 ustawy o usługach płatniczych. W rozpatrywanym przypadku pozwany bank nie wywiązał się z ich wypełnienia w stosunku do powoda. Gdyby bowiem zabezpieczenia transakcji elektronicznych stosowane przez pozwanego były właściwe, nie doszłoby do dokonania na rachunku powoda transakcji przez nieuprawnione do tego osoby trzecie.

Nadto, należy zwrócić uwagę na jeszcze jeden aspekt działania pozwanego, który budzi zastrzeżenia co do jego profesjonalizmu. Otóż, po zgłoszeniu przez powoda reklamacji pozwany zwrócił na rachunek powoda kwotę 30.186,71 zł, po czym następnie – po negatywnym rozpatrzeniu reklamacji – pobrał tę kwotę z rachunku. Tego typu działanie nie miało podstawy prawnej. Bank nie jest bowiem uprawniony do dowolnego i arbitralnego pobierania z rachunku posiadacza rachunku bankowego żadnych środków pieniężnych. W niniejszym przypadku powód nie złożył dyspozycji, nie wyraził zgody na pobranie tej kwoty z rachunku ani też nie wyraził takiej zgody w zawartej przez strony umowie. Nadto, brak podstawy do tego typu działań w ustawie o usługach płatniczych. Jeśli pozwany uważał, że powód umyślnie doprowadził do nieautoryzowanej transakcji płatniczej bądź dopuścił się wskutek rażącego niedbalstwa naruszenia któregokolwiek z obowiązków o których mowa jest w art. 42 ustawy o usługach płatniczych winien dochodzić zwróconej kwoty na drodze sądowej.

W świetle zebranego materiału dowodowego nie ulega wątpliwości, że powód niezwłocznie po zauważeniu utraty środków na koncie dokonał zgłoszenia nieautoryzowanych transakcji, a zatem dochował terminu o jakim mowa w art. 44 ust. 2 ustawy o usługach płatniczych.

Mając zatem na względzie wszystkie przytoczone powyżej okoliczności, na mocy art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011r. o usługach płatniczych, Sąd zasądził od pozwanego na rzecz powódki kwotę 30.186,71 zł. Nadto, na podstawie art. 481 k.c. Sąd zasądził odsetki ustawowe za opóźnienie od dnia 22 sierpnia 2020r. do dnia zapłaty, mając na względzie, że w dniu 22 lipca 2020r. powód złożył reklamację i wniosła o zwrot utraconych środków, w oparciu o ustawę z dnia 5 sierpnia 2015r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym. Roszczenie stało się wymagalne z upływem 30 – dniowego terminu, o jakim mowa w powołanej ustawie.

O kosztach procesu Sąd orzekł na mocy art. 98 k.p.c. i zgodnie z zasadą odpowiedzialności za wynik sprawy zasądził od przegrywającego niniejszą sprawę pozwanego na rzecz powodów kwotę 5.127 zł, na którą składają się: opłata sądowa od pozwu (1.510 zł), opłata za czynności fachowego pełnomocnika w stawce minimalnej (3.600 zł) oraz opłata skarbowa od pełnomocnictwa (17 zł).