Sygnatura akt II Ca 452/18

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 3 lipca 2018 roku

Sąd Okręgowy w Krakowie II Wydział Cywilny – Odwoławczy w składzie:

Przewodniczący: SSO Grzegorz Buła

Protokolant:

po rozpoznaniu w dniu 21 czerwca 2018 roku w Krakowie

na rozprawie

sprawy z powództwa T. N.

przeciwko (...) Bank (...) S.A. w W.

o zapłatę

na skutek apelacji powódki od wyroku Sądu Rejonowego dla Krakowa-Nowej Huty w Krakowie z dnia 29 września 2017 roku, sygnatura akt I C 827/16/N

1. zmienia zaskarżony wyrok w ten sposób, że:

a) zasądza od strony pozwanej (...) Bank (...) S.A. w W. na rzecz powódki T. N. kwotę 9000 zł (dziewięć tysięcy złotych) wraz z ustawowymi odsetkami od dnia 19 lipca 2014 roku do dnia 31 grudnia 2015 roku oraz z ustawowymi odsetkami za opóźnienie od dnia 1 stycznia 2016 roku do dnia zapłaty;

b) zasądza od strony pozwanej (...) Bank (...) S.A. w W. na rzecz powódki T. N. kwotę 1517 zł (tysiąc pięćset siedemnaście złotych) tytułem zwrotu kosztów procesu;

2. zasądza od strony pozwanej (...) Bank (...) S.A. w W. na rzecz powódki T. N. kwotę 1200 zł (tysiąc dwieście złotych) tytułem zwrotu kosztów postępowania apelacyjnego.

SSO Grzegorz Buła

Sygnatura akt II Ca 452/18

UZASADNIENIE

wyroku z dnia 3 lipca 2018 roku

Wyrokiem z dnia 29 września 2017 roku Sąd Rejonowy dla Krakowa – Nowej Huty w Krakowie oddalił powództwo T. N., w którym powódka domagała się zasądzenia od (...) Banku (...) Spółki Akcyjnej z siedzibą w W. kwoty 9 000 zł z ustawowymi odsetkami, liczonymi od dnia 19 lipca 2014 r. do dnia zapłaty, a także kosztami procesu. W punkcie II. wyroku Sąd Rejonowy dla Krakowa – Nowej Huty w Krakowie zasądził od powódki na rzecz strony pozwanej kwotę 1217 zł tytułem zwrotu kosztów procesu.

Sąd Rejonowy wskazał na okoliczności niesporne między stronami, a to:

- od 21 lipca 2011 r. wiązała je umowa rachunku oszczędnościowo-rozliczeniowego, usług bankowości elektronicznej oraz karty debetowej;

- szczegółowe warunki usług bankowych zawarte były w regulaminie – załączniku do uchwały zarządu Banku z dnia 25 stycznia 2011 r., który był powódce znany w chwili zawarcia umowy;

- w dniu 18 lipca 2017 r. niezidentyfikowana osoba trzecia złożyła za pośrednictwem bankowości elektronicznej zlecenie przelewu kwoty 9000 zł na obce konto (w tym samym Banku), podając dane dostępowe do konta powódki; przelew ten został zrealizowany natychmiast;

- pieniędzy powódka nie odzyskała do dnia zamknięcia rozprawy;

Nadto Sąd Rejonowy ustalił, że T. N. prowadzi działalność gospodarczą, jest z wykształcenia ekonomistą. W dniu 18 lipca 2014 r. powódka chciała sprawdzić stan swojego konta, weszła na stronę bankowości elektronicznej (...) i zalogowała się skutecznie do systemu, podając login i hasło. W tym momencie nastąpiło przerwanie połączenia, na ekranie pokazał się komunikat o konieczności odebrania poczty elektronicznej. Powódka uczyniła to, w skrzynce odbiorczej zastała nową wiadomość, którą uznała za informację od Banku. Zawartością e-maila był tylko link, który powódka otworzyła, licząc, że odnowi w ten sposób połączenie z serwisem transakcyjnym Banku. Ukazała się wówczas strona, łudząco podobna do zabezpieczonej strony logowania pozwanego Banku. Powódka wpisała w odpowiednie rubryki swój login i hasło, po chwili ukazał się komunikat „podaj kod nr 21", co też powódka uczyniła. Tego samego dnia po południu powódka otrzymała telefon z Banku, z pytaniem, czy zlecała przelew na kwotę 9000 zł. Gdy zaprzeczyła, poradzono jej, by złożyła reklamację drogą mailową. Powódka nigdy wcześniej nie otrzymywała od banku wiadomości elektronicznych, zawierających link do strony logowania. Nie podawała też wcześniej kodu z karty zdrapek przy operacji samego logowania, a jedynie przy zleceniach obciążających konto.

Wyłudzenia danych drogą mailową przez „podstawione" strony logowania, stanowiły proceder, który w 2014 r. rozwijał się na całym świecie; był zatem znany instytucjom finansowym, ogółowi ich klientów, jak również nagłaśniany przez media. Pozwany Bank z początkiem 2014 r. umieścił na internetowej stronie bankowości elektronicznej, u dołu formularza logowania, informację o zagrożeniu fałszywymi mailami, wyłudzającymi wrażliwe dane. W osobnej zakładce, dostępnej ze strony logowania, zawarte były zasady bezpiecznego korzystania z bankowości elektronicznej, w tym ostrzeżenia przez mailami, podszywającymi się pod Bank. Nadto, autentyczna strona logowania, jaką dysponuje strona pozwana, jest opatrzona unikatowym adresem, którego struktura – na początku wizerunek zamkniętej zielonej kłódki i symbol szyfrowania protokołu: https:\\ - potwierdza bezpieczeństwo transmisji. Adres ten nie może być wykorzystany przez żaden inny podmiot, dlatego strony internetowe „podstawiane" przez oszustów są opatrzone innymi adresami, często długimi i nietypowymi.

W regulaminie, stanowiącym załącznik do umowy rachunku bankowego, Bank zastrzegł m.in., że posiadacz rachunku jest zobowiązany do zachowania w tajemnicy informacji zapewniających bezpieczne korzystanie z rachunku(...) w szczególności numeru klienta, kodów jednorazowych, haseł dostępu oraz danych osobowych (§31 ust. 2 – k. 77). W§32 regulaminu Bank zastrzegł sobie uprawnienie do wykorzystania dodatkowego narzędzia autoryzacji, jakim jest identyfikacja klienta przez telefon.

Sąd Rejonowy jako fakty notoryjne wskazał też, że powszechnie wiadomo było w 2014 r. jakich metod używają hakerzy w celu nieuprawnionego transferu środków z cudzych rachunków bankowych.

Opisany stan faktyczny był w przeważającej części niesporny. Został tylko uzupełniony i doprecyzowany na podstawie zgromadzonych w aktach sprawy dokumentów: zawartej umowy, regulaminu, przesyłanej korespondencji, nagrania rozmowy telefonicznej. Nie budziły one zastrzeżeń Sądu, były zaakceptowane przez strony i stanowią wartościowy materiał dowodowy. Istotnym, przesądzającym o wyniku sprawy dowodem były zeznania powódki, która dokładnie opisała kolejne czynności, prowadzące do ujawnienia oszustom wrażliwych danych.

Sąd Rejonowy ocenił, że powództwo nie może odnieść zamierzonego skutku. Powódka opierała swoje żądanie na zarzucie niewłaściwego wykonania przez stronę pozwaną zobowiązania wynikłego z umowy rachunku bankowego. Zobowiązanie to polega m.in. na ochronie środków pieniężnych zdeponowanych przez klienta (zgodnie z regułami depozytu nieprawidłowego) przed ich wypłatą lub przelewem na rzecz osoby nieuprawnionej.

Sąd Rejonowy zauważył, że stosowany przez Bank w 2014 r. trzystopniowy system zabezpieczeń elektronicznego dostępu do konta (zaszyfrowana strona logowania, konieczność podania identyfikatora - hasła - a przy transakcjach „wrażliwych" - również kodu z karty) był na tyle bezpieczny i pewny, że przestępcy nie chcieli lub nie potrafili pokonać go bezpośrednio, bez aktywnego udziału posiadacza konta. Już same twierdzenia pozwu wskazują, że środki na rachunku powódki były nienaruszone do czasu, gdy ona sama nie ujawniła kodów dostępu osobom trzecim. W ocenie Sądu Rejonowego oznacza to, że słabym ogniwem całej oszukańczej transakcji nie były zabezpieczenia dostępu do konta (które nie zostały złamane), ale fakt ujawnienia tych zabezpieczeń przez powódkę osobie trzeciej. Z pewnością wśród zobowiązań wynikłych z umowy rachunku bankowego z elektronicznym dostępem do konta można odnaleźć obowiązek Banku do należytego informowania posiadaczy rachunków o zagrożeniach związanych z ujawnianiem haseł i kodów, a także - o istniejących w obrocie sposobach ich wyłudzania przez cyberprzestępców. Obowiązek ten, nawet jeśli nie wyrażony bezpośrednio w treści umowy albo przepisów prawa, wyprowadzić można z samej zasady lojalności kontraktowej i powinności ochrony konsumenta przez podmiot silniejszy ekonomicznie (art. 56 k.c.). Można było zatem wymagać od strony pozwanej, by podjęła odpowiednie działania informacyjne, które ustrzegą klientów przed ujawnianiem wrażliwych danych. W ocenie Sądu Rejonowego Bank ten obowiązek spełnił. Zamieszczenie wyraźnego ostrzeżenia o fałszywych e-mailach na stronie logowania do serwisu transakcyjnego - czyli w miejscu szczególnie eksponowanym - stanowiło prawidłowe i lojalne zachowanie wobec kontrahenta. Zapoznania się z treścią tak wyraźnego ostrzeżenia można wymagać od każdego przeciętnego obywatela. Powódka, trudniąca się działalnością gospodarczą i zawodu ekonomistka, nie tylko zapomniała to uczynić, ale też - jak ocenia Sąd - w momencie ataku oszustów nie zachowała podstawowej nawet ostrożności, za to bezrefleksyjnie realizowała polecenia wyświetlane na ekranie komputera. Jak powódka sama przyznała, tego dnia chciała jedynie odczytać stan konta, a przecież nigdy wcześniej nie była pytana o kod z karty przy tego rodzaju czynności (a jedynie przy zlecaniu transakcji obciążających rachunek). Również nigdy wcześniej nie logowała się do serwisu transakcyjnego via e-mail. O braku rozwagi świadczy również i to, że T. N. - po tym, jak fałszywy e-mail zniknął z jej skrzynki pocztowej - nie pomyślała nawet, by zwrócić się o pomoc w identyfikacji nadawcy (lub jego hosta) do firmy, która obsługiwała jej korespondencję elektroniczną (tak zeznania powódki k. 178). Omawiane postępowanie stanowiło jednocześnie naruszenie zobowiązania klienta do zachowania swoich danych w tajemnicy (powołany wcześniej art. 31 ust. 2 regulaminu).

W świetle ustalonego stanu faktycznego Sąd Rejonowy uznał, że pozwany Bank zastosował metody zabezpieczeń adekwatne do rodzaju prowadzonego konta, zgodne z aktualną wiedzą i z zachowaniem szczególnej staranności, o jakiej mowa w art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997 r. - prawo bankowe (tekst jednolity: Dz. U. z 2002 r. Nr 72, poz. 665 ze zm.)., a jedyną przyczyną ujawnienia danych, które pozwoliło oszustom na dostęp do środków pieniężnych, było obiektywnie wadliwe zachowanie powódki. Trudno też uznać, by stosowane przez Bank zabezpieczenia miały wadę takiego rodzaju, która to ujawnienie w jakiś sposób ułatwiła. Warto zauważyć, że nawet ustalona z góry kolejność podawania kodów z karty (obecnie zastąpiona metodą losowania numeru kodu przez system) w realiach niniejszej sprawy nie ułatwiała wcale oszustwa. Istotą phishingu jest bowiem najpierw wyłudzenie danych, które pozwalają atakującemu natychmiast zalogować się na dane konto, a kolejne pytanie o kod zadawane jest już bezpośrednio z poziomu logowania (oszust, zalogowany jako posiadacz rachunku, zleca przelew i otrzymuje od Banku pytanie o kod nr „x" z karty kodów, pytanie to przesyła w formie „wyskakującego okienka" do posiadacza rachunku, a informacje zwrotną wpisuje we właściwą rubrykę). Przekonanie powódki, że pytanie o właściwy kolejny numer kodu może pochodzić tylko od Banku, było zatem oparte na nieadekwatnej i powierzchownej ocenie sytuacji.

Wynika stąd, że pomiędzy działaniem czy zaniechaniem pozwanego a utratą środków z konta bankowego nie zachodzi adekwatny związek przyczynowy, przeciwnie - przyczyną szkody jest niewłaściwe wykonanie umowy przez powódkę.

Zdaniem Sądu Rejonowego powódka trafnie argumentuje, że umowa rachunku bankowego rodzi po stronie instytucji finansowej zobowiązanie rezultatu: wpłacone środki pieniężne stają się przejściowo własnością banku, który ponosi ryzyko ich utraty, w tym przez wypłacenie niewłaściwej osobie. Z drugiej strony bank jest obowiązany wykonywać wszelkie zlecenia posiadacza rachunku dotyczące zdeponowanych środków (art. 50 ust. 2 ustawy -prawo bankowe), a za niewykonanie zlecenia ponosi odpowiedzialność kontraktową na zasadach ogólnych. Wynika stąd, że surowa odpowiedzialność prowadzącego rachunek za depozyt pieniężny trwa do chwili, w której bank wykona dyspozycję wypłaty bądź przelewu środków zgodnie z życzeniem posiadacza tego rachunku. Zdaniem Sądu Rejonowego odróżnić trzeba przy tym sytuację, w której wypłata środków dokonana jest na rzecz osoby nieuprawnionej bez jakiegokolwiek udziału posiadacza rachunku (przy użyciu zgubionej czy ukradzionej karty kredytowej, wskutek sfałszowania czeku) od sytuacji, gdy posiadacz rachunku bierze aktywny udział w transakcji wypłaty. W niniejszej sprawie kluczowe jest, że powódka brała czynny udział w zleceniu przelewu. Zalogowała się bowiem świadomie na konto za pomocą loginu i hasła, a następnie podała kod, umożliwiający dokonanie przelewu (wypłaty) środków. Wprawdzie powódka twierdzi, że tej ostatniej czynności nie chciała dokonać, ale z punktu widzenia art. 60 k.c. oświadczenie woli o treści „uzupełnionej" przez oszustów zostało przez nią złożone. W polskim systemie prawa prywatnego przyjęto mieszaną teorię oświadczenia woli, która uznaje za wiążące każde zachowanie osoby, które dostatecznie jasno wyraża wolę wywołania określonych skutków prawnych. Jeżeli zatem ktoś nieostrożnie składa podpis pod umową nie znając nawet jej treści, jego zachowanie jest równoważne zawarciu całej umowy ze wszystkimi tego skutkami. Sytuacja rozpoznawana w niniejszej sprawie jest zdaniem Sądu analogiczna. Powódka skutecznie uczestniczyła w zleceniu przelewu, które z punktu widzenia banku było wiążące i skutkowało wypłatą środków z konta. Dokonanie tej wypłaty zgodnie z oświadczeniem woli powódki zwalnia jednocześnie bank z odpowiedzialności za zwrot środków pieniężnych złożonych w depozycie.

Wbrew twierdzeniom powódki, zlecenie przelewu nie mogło być przez nią skutecznie odwołane bez zgody adresata oświadczenia woli - art. 61§1 k.c. Bank słusznie wskazał, że możliwe jest odwoływanie przelewów jeszcze niewykonanych. Że jednak sporna transakcja została wykonana od razu, między rachunkami w tym samym banku, nie można było jej cofnąć bez udziału posiadacza rachunku, na którym nastąpiło uznanie.

O kosztach procesu Sąd Rejonowy orzekł na zasadzie odpowiedzialności za jego wynik (art. 98§1 i§3 k.p.c. w zw. z art. 99 k.p.c.).

Powyższy wyrok apelacją zaskarżyła powódka T. N., domagając się jego zmiany i orzeczenia zgodnie z pozwem, ewentualnie uchylenia wyroku i przekazania sprawy do ponownego rozpoznania. Zarzuciła naruszenie:

1. art. 845 k.c. w zw. z art. 60 k.c. poprzez bezpodstawne przyjęcie, że dokonana operacja na rachunku bankowym powódki, efektem której był przelew na kwotę 9 000 zł, miała charakter autoryzowany przez powódkę i została podjęta zgodnie z wolą posiadacza rachunku, obciążając skutecznie rachunek powódki, a nie bank,

2. art. 233 § 1 k.p.c. w zw. z art. 56 k.c., art. 228 k.p.c. i art. 235 k.p.c. poprzez naruszenie zasady swobodnej oceny dowodów, a wskutek tego uznanie za notoryjne faktów związanych ze sposobami dokonywania wyłudzeń danych w okresie 2014 r., które rzekomo miały być znane nie tylko instytucjom finansowym, ale także ich klientom, nie przeprowadzenie dowodu z akt sprawy Komendy Powiatowej Policji w (...) D-964 S/14 dotyczącej setek wyłudzeń danych z kont klientów Banku (...) w 2014 r., pomimo naprowadzonego i uznanego przez Sąd Rejonowy za notoryjny fakt znajomości przez klientów pozwanego baku zagrożeń oraz rzekomego informowania ich o tych zagrożeniach przez bank, a w końcu uznanie, że wskutek stosowanych (pozytywnie ocenionych przez Sąd) procedur bank zwolniony jest z odpowiedzialności w stosunku do powódki, także z tego powodu, że wypełnił swoje obowiązki informacyjne.

Skarżący zwrócił uwagę na treść art. 45 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, z którego wynika, że ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez powódkę spoczywa na banku (pozwanym). Samo wykazanie przez bank użycia instrumentu płatniczego nie jest wystarczające. O braku woli autoryzacji przez powódkę takiej transakcji świadczy niezwłoczne złożenie reklamacji po otrzymaniu od banku informacji o powstałym problemie oraz zawiadomienie Policji. Zdaniem apelującego bank nie wykazał winy umyślnej powódki

w doprowadzeniu do nieautoryzowanej transakcji, jak również nie udowodnił, że wskutek rażącego niedbalstwa dopuściła się powódka naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych.

W odpowiedzi na apelację strona pozwana wniosła o jej oddalenie oraz zasądzenie na swoją rzecz zwrotu kosztów postępowania według norm przepisanych.

Sąd Okręgowy zważył, co następuje:

Apelacja jest zasadna.

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 za notoryjne niektórych elementów stanu faktycznego. W ocenie Sądu Okręgowego nie są oczywiste okoliczności, że dokładnie w tym okresie miały miejsce ataki tożsame z tym, którego ofiarą stała się powódka, że informacje o nich podawano do publicznej wiadomości i były to fakty powszechnie znane. Oczywiście rynek usług bankowości elektronicznej stale się rozwija i świadomość jego klientów na dzień dzisiejszy z pewnością większa, jednak Sąd Okręgowy nie podziela przekonania Sądu Rejonowego, że w 2014 r. metody działania hakerów i środki obrony przed nimi były powszechnie znane.

W ocenie Sądu Okręgowego, za trafne ponadto należało uznać zarzuty niewłaściwej oceny prawnej ustaleń faktycznych. W uzasadnieniu zaskarżonego rozstrzygnięcia Sąd Rejonowy nie powoływał wprost podstawy prawnej orzeczenia – wydaje się jednak, że opierał je w regulacjach dotyczących umowy rachunku bankowego w powiązaniu z odpowiedzialnością odszkodowawczą. W szczególności zasadnie skarżący zarzuca brak odniesienia dochodzonego roszczenia do treści ustawy z dnia 19 sierpnia 2011 roku 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 u.u.p. zamieszczono tzw. słownik zawierający objaśnienia określeń ustawowych, co pozwala na identyfikację stron stosunku prawnego – powódki 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 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.

Przenosząc powyższe rozważania na grunt niniejszej sprawy wskazać należy, że ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową. Ma to ten skutek, że równoległą podstawą odpowiedzialności banku jest ustawa o usługach płatniczych z dnia 19 sierpnia 2011 r. Ustawa ta przewiduje generalną zasadę, że dostawca ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika. Zgodnie z art. 46 ust. 1 powołanej ustawy w przypadku wystąpienia nieautoryzowanej transakcji płatniczej, dostawca płatnika jest obowiązany niezwłocznie dokonać na rzecz płatnika zwrotu kwoty nieautoryzowanej transakcji płatniczej albo, w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcją płatnicza. Art. 45 ust. 1 powołanej ustawy stanowi, że ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika spoczywa na dostawcy tego użytkownika, przy czym do zrealizowania tego obowiązku dowodowego nie jest wystarczające wykazanie samego zarejestrowanego użycia instrumentu płatniczego. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie i wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 u.u.p.

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 powódki. 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 powódki transakcji przez nieuprawnione do tego osoby.

Trafne są zarzuty apelacji, że powódka jako klient banku nie naruszyła obowiązków, o których mowa w art. 42 umyślnie lub wskutek rażącego niedbalstwa. Z pewnością działanie powódki nie było umyślne, skoro jej zamiarem w ogóle nie było dokonywanie jakichkolwiek operacji na rachunku, a jedynie sprawdzenie stanu środków. Zdaniem Sądu Okręgowego powódce nie można również przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa. Komputer powódki posiadał zainstalowane oprogramowanie antywirusowe. Powódka nie udostępniała świadomie identyfikatora, hasła ani innych danych osobom trzecim. W dniu 18 lipca 2014 roku powódka wykonywała pewne czynności w systemie bankowości internetowej, jednak dokonanie przelewu kwoty 9 000 zł z rachunku bankowego powódki nastąpiło poza jej wiedzą i bez autoryzacji przez powódkę. Doszło wprawdzie do potwierdzenia transakcji za pomocą właściwego narzędzia, jednak użycie kolejnego kodu z karty kodów nie nastąpiło z nastawieniem wyrażenia zgody na dokonanie przelewu. Kod został wpisany przez powódkę w innym celu, a osoba trzecia posłużyła się nim w sposób nieuprawniony do potwierdzenia transakcji. Już w toku postępowania reklamacyjnego powódka zaprzeczyła, by doszło do autoryzacji usługi, a przeciwne okoliczności zgodnie z rozkładem ciężaru dowodu nie zostało wykazane przez stronę pozwaną. Jest niewątpliwie uchybieniem po stronie powódki, że niezbyt precyzyjnie weryfikowała komunikaty na ekranie komputera, w pewnym zakresie z pewnością działaniu powódki można postawić zarzut nienależytej staranności. 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 powódki, które zaistniały nie mogą być kwalifikowane jako rażące niedbalstwo.

Z powyższych względów Sąd Okręgowy zmienił zaskarżone orzeczenie zgodnie z art. 386 § 1 k.p.c., zasądzając na rzecz powódki od strony pozwanej kwotę 9 000 zł wraz z ustawowymi odsetkami od dnia 19 lipca 2014 r. do dnia 31 grudnia 2015 r. oraz z ustawowymi odsetkami za opóźnienie od dnia 1 stycznia 2016 r. do dnia zapłaty. O kosztach procesu za obie instancję orzeczono zgodnie z zasadą odpowiedzialności za jego wynik wyrażoną w art. 98 k.p.c.

SSO Grzegorz Buła