



**Rzecznik
Finansowy**

www.rf.gov.pl

dr Bohdan Pretkiel

Warszawa, dnia [REDACTED]

[REDACTED]

Rzecznik Finansowy
ul. Nowogrodzka 47 A
00-695 Warszawa

Sąd [REDACTED]

w [REDACTED]

ul. [REDACTED]

Powódka:

[REDACTED]

zastępowana przez:

r.pr. [REDACTED]

(adres stron w aktach sprawy)

Pozwany:

[REDACTED]

zastępowany przez:

r.pr. [REDACTED]

adw. [REDACTED]

(adres stron w aktach sprawy)

Sygnatura akt: [REDACTED]

Rzecznik Finansowy
Ul. Nowogrodzka 47A
00-695 Warszawa

@ biuro@rf.gov.pl
www.rf.gov.pl
f facebook.com/Rzecznik
Finansowy

☎ Tel. 22 333 73 26
22 333 73 27
fax. 22 333 73 29

Oświadczenie Rzecznika Finansowego zawierające pogląd istotny dla sprawy:

Zgodnie z art. 28 ustawy z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego, o Rzeczniku Finansowym i o Funduszu Edukacji Finansowej (t.j. Dz. U. z 2022 r. poz. 187; zm., dalej: ustawa o Rzeczniku Finansowym), *do Rzecznika stosuje się odpowiednio przepis art. 63 ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego (Dz. U. z 2021 r. poz. 1805, 1981 i 2052)*. Z kolei, zgodnie z art. 63 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2021 r. poz. 1805, z późn. zm.; dalej: k.p.c.), *Organizacje pozarządowe wymienione w artykułach poprzedzających, które nie uczestniczą w sprawie, mogą przedstawiać sądowi istotny dla sprawy pogląd wyrażony w uchwale lub w oświadczeniu ich należycie umocowanych organów*.

W dniu [REDAKTOR] r. do Rzecznika Finansowego wpłynął wniosek z dnia [REDAKTOR] r. Pani [REDAKTOR] (dalej: powódka) sporządzony przez profesjonalnego pełnomocnika r.pr. [REDAKTOR] z prośbą o przedstawienie sądowi oświadczenia Rzecznika Finansowego zawierającego pogląd istotny dla sprawy wniesionej z jej powództwa przeciwko [REDAKTOR] (dalej: pozwany lub Bank; łącznie dalej: Strony) – kopia wniosku wraz z kopią pełnomocnictwa stanowią załącznik nr 1 do niniejszego pisma.

Mając powyższe na uwadze oraz działając na podstawie art. 28 ustawy o Rzeczniku Finansowym w zw. z art. 63 k.p.c., niniejszym Rzecznik Finansowy przedstawia sądowi oświadczenie zawierające pogląd istotny dla przedmiotowej sprawy.

Uzasadnienie:

Za podstawę opracowania niniejszego poglądu przyjęto:

1. wniosek o wydanie istotnego poglądu w sprawie z dnia [REDAKTOR] r.;
2. pozew o zapłatę z dnia [REDAKTOR] r. wraz z załącznikami;
3. odpowiedź na pozew z dnia [REDAKTOR] r. wraz z załącznikami;
4. pismo w sprawie Pozwanego z dnia [REDAKTOR] r. wraz z załącznikiem;
5. pismo przygotowawcze Powódki z dnia [REDAKTOR] r.

Str. 2

I. Treść i zakres istotnego poglądu

Jedną z podstawowych kwestii dla rozstrzygnięcia przedmiotowego sporu, w ocenie Rzecznika Finansowego, stanowi udzielenie odpowiedzi na poniższe pytania:

1. która ze stron umowy (i w jakim wymiarze) ponosi odpowiedzialność z tytułu dokonania nieautoryzowanych transakcji płatniczych (za pośrednictwem bankowości elektronicznej) w okolicznościach przedmiotowej sprawy w świetle przepisów ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (tekst jedn. Dz. U. z 2021 r. poz. 1907¹, z późn. zm., dalej „UUP”) oraz ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (tekst jedn. Dz. U. z 2021 r. poz. 2439², z późn. zm., dalej „Prawo bankowe”);
2. i w kontekście powyższego ustalenie, czy płatnikowi (powódce) – w okolicznościach będących przyczyną zawisłego między stronami sporu – można przypisać doprowadzenie do nieautoryzowanych transakcji w wyniku będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 UUP, co eliminowałoby odpowiedzialność Banku z tytułu dokonania nieautoryzowanej transakcji płatniczej,
3. a także w jaki sposób rozkłada się ciężar odpowiedzialności obu stron w świetle art.45 oraz art. 46 UUP w odniesieniu do okoliczności przedmiotowej sprawy.

Niniejsze oświadczenie Rzecznika Finansowego stanowić będzie zatem szersze omówienie aspektu rozkładu odpowiedzialności z tytułu dokonania nieautoryzowanych transakcji płatniczych w rozumieniu UUP.

II. Odniesienie się do pozwu i odpowiedzi na pozew

Z punktu widzenia prawidłowej oceny okoliczności analizowanej sprawy należy uznać, że immanentnym jej aspektem jest konieczność dokonania gruntownej analizy wybranych przepisów Działu III, Rozdziału 2 UUP, w których unormowano materię autoryzacji transakcji

¹ Stan prawny na dzień wykonania nieautoryzowanych transakcji.

² Jak wyżej.

płatniczych oraz odpowiedzialności stron umowy ramowej o świadczenie usług płatniczych z tytułu dokonania nieautoryzowanych transakcji.

Jako ww. umowę ramową pomiędzy stronami należy traktować umowę ramową o korzystanie z systemu bankowości internetowej, a także jej integralną część Regulamin świadczenia usług Systemu bankowości internetowej [REDACTED] obowiązujący w dniu dokonania przedmiotowych transakcji płatniczych. Wymaga na tym etapie podkreślenia, że na podstawie art. 8 ust. 1 UUP ustawodawca przyjął, że postanowienia umów (a tym samym regulaminów) o usługi płatnicze nie mogą być mniej korzystne dla użytkowników niż przepisy ustawy, chyba że ustawa stanowi inaczej. Wszystkie zatem postanowienia umowy oraz regulaminu, wiążących powódkę oraz pozwaną Bank, należy rozpatrywać przez pryzmat zgodności z przepisami tej ustawy. Postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy są nieważne; zamiast nich stosuje się odpowiednie przepisy ustawy³.

Jak wynika z przedstawionych Rzecznikowi akt przedmiotowej sprawy, w dniu [REDACTED] r. z rachunku bankowego powódki dokonano transakcji płatniczych – wypłat w bankomacie Euronet poprzez usługę BLIK na łączną kwotę 3.000,00 zł (3 x 1.000,00 zł) oraz płatności BLIK na rzecz Skinport GmbH w kwotach: 1.800,18 zł, 2.102,96 zł i 1.838,97 zł.

Z analizy przedmiotowej dokumentacji (odpowiedzi na pozew) wynika, że pozwany Bank wprost wskazuje na możliwy udział osób trzecich (oszustów) w odniesieniu do dokonania spornej transakcji płatniczej (powołując się na rażące niedbalstwo ze strony powódki jako przyczynę odmowy zwrotu środków), co oznacza niekwestionowanie faktu rzeczywistego zlecenia i dokonania ich przez te osoby (osobę), co już *per se* oznacza, że transakcje te należałoby uznać za nieautoryzowane. Oznacza to, że powódka najprawdopodobniej padła ofiarą kompleksowo przeprowadzonych oszukańczych działań ze strony przestępców, które polegały na kradzieży danych oraz stosownych danych

³ Art. 8 ust. 2 UUP

uwierzytelniających, być może również na skutek zastosowanych zabiegów socjotechnicznych, związanych z manipulacją ofiarą (*phishing*).

Odnosnie twierdzeń pozwanego Banku, sugerujących możliwość przypisania powódce działania, które wyczerpuje znamiona art. 42 ust. 2 UUP również – w ocenie Rzecznika Finansowego – należy wskazać, że trudno mówić w tej sytuacji o braku zadośćuczynienia tym przepisom. Należy bowiem mieć na uwadze, że powódka mogła paść ofiarą przestępstwa i oszukańczych działań przestępców. Powódka działała w przeświadczeniu, że pozostaje w środowisku bankowości elektronicznej Banku i loguje się do strony Banku (korzysta w sposób standardowy z usług Banku) i wszelkie czynności, które wykonuje, związane są z realizacją umowy, a więc pomiędzy nią oraz Bankiem. Jej celem było prawdopodobnie dokonanie standardowych operacji w związku z korzystaniem z bankowości elektronicznej, jednak na skutek oszukańczych działań ze strony przestępców doszło m.in. do wyłudzenia danych uwierzytelniających i kodów BLIK.

Trudno w takim wypadku mówić o:

- a) świadomym i zawinionym naruszeniu przez powódkę indywidualnych zabezpieczeń instrumentu płatniczego,
- b) świadomym nieprzechowywaniu instrumentu płatniczego z zachowaniem należytej staranności,
- c) czy wreszcie świadomym udostępnianiu go osobom nieuprawnionym.

Zachowanie powódki można co najwyżej rozpatrywać jako nieumyślne udostępnienie danych uwierzytelniających, związanych z korzystaniem z instrumentu płatniczego, osobom nieuprawnionym (a właściwie wyłudzenie od niej tych danych), jednak wówczas ustalenia przez sąd wymaga – zgodnie z art. 46 ust. 3 UUP - czy było to efektem rażącego niedbalstwa. Istota art. 46 ust. 3 UUP polega więc na tym, że płatnik nie będzie ponosił pełnej odpowiedzialności za każde udostępnienie instrumentu płatniczego osobom trzecim. W takim wypadku zasadą będzie jego odpowiedzialność do równowartości 50 euro (art. 46 ust. 2 UUP). Natomiast tylko wówczas, gdy umyślnie lub wyniku rażącego niedbalstwa udostępni instrument płatniczy osobom nieuprawnionym, odpowiadać będzie w pełnej wysokości.

Oznacza to też, że w tych wszystkich wypadkach, w których udostępnienie to będzie wynikać nawet z niedbałego zachowania płatnika, nie będzie można automatycznie przypisać płatnikowi (powódce) pełnej odpowiedzialności, gdyż będzie to możliwe dopiero wówczas, gdy niedbałość ta cechować się będzie stopniem rażącym.

Wymaga także podkreślenia w rezultacie powyższych uwag oraz treści pism procesowych, że w ocenie Rzecznika zasadniczym przedmiotem rozstrzygnięcia nie jest fakt dokonania nieautoryzowanych transakcji w sensie faktycznym. Oś sporu stanowi w tym wypadku ustalenie odpowiedzialności z tytułu dokonania nieautoryzowanych transakcji płatniczych, a precyzując – możliwość obciążenia skutkami jej dokonania powódki w świetle przepisów UUP. W ocenie Rzecznika Finansowego kwestia ta jest niezwykle istotna z punktu widzenia dokonania prawidłowego rozstrzygnięcia.

W świetle przedmiotowego sporu należy również wskazać, że Powódka nie przekazała dobrowolnie danych oszustom, a została prawdopodobnie w profesjonalny sposób oszukana i zmanipulowana, a indywidualne dane uwierzytelniające (kody autoryzacyjne) zostały od niej wyłudzone. Jest to zasadnicza różnica w odniesieniu do tego, co twierdzi pozwany. Wymaga także udzielenia odpowiedzi na pytanie, czy w sytuacji, w której *de facto* zlecenie płatnicze składane jest przez oszusta z wykorzystaniem wyłudzonych danych od klienta, a nie przez tego klienta, to klient autoryzuje tę transakcję, a więc składa w pełni świadome oświadczenie woli i wiedzy o jej wykonaniu, czyli wyraża na nią zgodę? Powódka pozostawała w stanie nieświadomości, że na jej rachunku dokonywane są jakiegokolwiek transakcje przelewu środków z użyciem kodów BLIK.

Jeśli zatem przyjęte zostanie, że powódka padła ofiarą przestępców i to *de facto* oni dokonali złożenia zleceń płatniczych (tj. to przestępcy *de facto* kontaktowali się z pozwanym Bankiem i to oni składali zlecenia na podstawie danych uzyskanych od powódki, a więc to oni składali oświadczenia woli, nie zaś powódka), w rezultacie których wykonano sporne transakcje płatnicze (obciążenie rachunku płatniczego), to trudno w takich okolicznościach uznać, iż to powódka wyraziła zgodę na dokonanie oszukańczej transakcji (w rozumieniu prawa cywilnego – czyli złożyła oświadczenie woli), tj. wyraziła rzeczywistą wolę jej wykonania.

W tym kontekście warto wskazać, że zgodnie z rekomendacją KNF⁴: „Dostawcy usług płatniczych powinni stosować mechanizmy monitorowania transakcji mające na celu zapobieganie nielegalnym/oszukańczym transakcjom oraz wykrywanie i blokowanie takich transakcji płatniczych przed wykonaniem przez dostawcę usługi płatności internetowej. Transakcje podejrzane lub wysokiego ryzyka powinny podlegać szczególnej procedurze kontroli i oceny”⁵. Ponadto, zgodnie z rekomendacją pkt 10.1. zd. 1: „Dostawcy usług płatniczych powinni stosować systemy wykrywania i zapobiegania oszustwom w celu identyfikacji podejrzanych transakcji przed wykonaniem przez dostawcę usługi płatności internetowej”⁶.

Należy podkreślić, że obowiązki banku w tym zakresie nie wynikają jedynie z ww. rekomendacji KNF. W tym kontekście warto również przytoczyć treść art. 41 ust. 2 UUP, zgodnie z którym: „W umowie ramowej można zastrzec prawo dostawcy do blokowania instrumentu płatniczego:

- 1) z uzasadnionych przyczyn związanych z bezpieczeństwem instrumentu płatniczego,
- 2) w związku z podejrzeniem nieuprawnionego użycia instrumentu płatniczego lub umyślnego doprowadzenia do nieautoryzowanej transakcji płatniczej lub
- 3) z powodu zwiększenia ryzyka utraty przez płatnika zdolności kredytowej wymaganej dla danego instrumentu płatniczego, gdy korzystanie z instrumentu płatniczego jest związane z korzystaniem przez płatnika z udzielonego mu kredytu”.

Natomiast zgodnie z art. 41 ust. 3 UUP: „Dostawca powinien poinformować płatnika, w uzgodniony sposób, o zablokowaniu instrumentu płatniczego przed zablokowaniem tego instrumentu, a jeżeli nie jest to możliwe – niezwłocznie po jego zablokowaniu. Nie dotyczy to

⁴ Rekomendacja Komisji Nadzoru Finansowego (KNF) z listopada 2015 r. dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo – kredytowe https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczyc_h_43526.pdf

⁵ Rekomendacja 10 Rekomendacji KNF, str. 20.

⁶ Rekomendacja 10.1. zd. 1 Rekomendacji KNF, str. 20.

przypadków, gdy przekazanie informacji o zablokowaniu instrumentu byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów”.

Co oczywiste, zablokowanie instrumentu i poinformowanie płatnika powinno nastąpić przed wykonaniem transakcji, a więc wówczas, gdy istnieje „*podejrzenie nieuprawnionego użycia instrumentu płatniczego*” – w przeciwnym razie byłoby to bowiem bezcelowe.

Biorąc pod uwagę twierdzenia pozwanego Banku, wymaga podkreślenia, że istnieje prawdopodobieństwo, iż powódka stała się ofiarą przestępstwa, nie na skutek lekkomyślności (ani na skutek rażącego niedbalstwa – *vide* przesłanka wynikająca z art. 46 ust. 3 UUP), a właśnie z powodu profesjonalnie przygotowanego przestępstwa, którego celem było najpierw pozyskanie danych uwierzytelniających, a następnie kradzież środków zgromadzonych na rachunku przy użyciu bankowości elektronicznej. Wydaje się, że trudno rozpatrywać zagadnienie lekkomyślności oraz jej szczególnej kwalifikowanej postaci, czyli rażącego niedbalstwa, jeśli *de facto* stroną czynną nie była tu powódka (nie ujawniła swoich danych publicznie, na forum itd.), a przestępcy, którzy podszywali się pod Bank po prostu dokonali oszustwa.

Pozwany Bank wskazuje, że strona powodowa zignorowała obowiązujące w Banku zasady bezpieczeństwa bankowości elektronicznej. W ocenie Rzecznika Finansowego ponownie wymaga podkreślenia w tym kontekście, że nieracjonalnym byłoby przyjmowanie takich wniosków w sytuacji, gdy osoba logująca się do swojego systemu bankowości elektronicznej i podająca kody autoryzacyjne w tym celu, ignorowała obowiązujące w Banku zasady bezpieczeństwa, skoro działała w przeświadczeniu, że podejmuje te czynności właśnie w ramach standardowej relacji z Bankiem (a w rzeczywistości na skutek *de facto* oszukańczych działań przestępców). Powstaje zatem pytanie, czy takie zachowanie wypełnia przymiot „*rażącego niedbalstwa*”.

Do oceny tut. Sądu należy zatem pozostawić kwestię, czy w okolicznościach sprawy powódki można ewentualnie mówić o wyższym stopniu zwykłego niedbalstwa, leżącego już bardzo blisko winy umyślnej w sytuacji, gdy padła ona ofiarą profesjonalnie przygotowanych działań przestępczych oszustów, których celem była tylko i wyłącznie kradzież danych oraz środków z rachunku. Należy bowiem pamiętać, że tylko w przypadku przypisania powódce

przymiotu „rażącego niedbalstwa” – zgodnie z art. 46 ust. 3 UUP – ponosi ona pełną odpowiedzialność z tytułu dokonania przedmiotowych nieautoryzowanych transakcji.

Sąd Okręgowy w Warszawie rozpatrując roszczenie z tytułu nieautoryzowanych transakcji odwołał się do tej kwestii wskazując następująco: *„Brak wiedzy umożliwiającej odróżnić wrogie oprogramowanie od autentycznego przy pierwszym jego użyciu nie może stanowić podstawy do przypisania nieprofesjonalistycznie przymiotu rażącego niedbalstwa. Zdaniem Sądu Okręgowego, żeby można było stwierdzić, że coś jest "rażące", to musi być obiektywnie czyli powszechnie oczywiste, a w tej sprawie oceniane zachowanie dotyczyło stanu i treści systemu internetowego, które dla zwykłego użytkownika systemu komputerowego nie są ani niczym obiektywnym, ani oczywistym. Przeciętny użytkownik internetu, który po raz pierwszy posługuje się nową aplikacją nie jest w stanie odróżnić właściwej aplikacji od tej zawirusowanej, nie wiedząc różnicy graficznej w ich treści i obrazie. Dlatego w tych okolicznościach sprawy sam fakt, że powód przyznał, że znał zagrożenia z informacji skierowanej przez bank do ogółu klientów, nie stanowiło okoliczności pozwalających na zakwalifikowanie instalacji wrogiego oprogramowania za czynność kwalifikowaną w kategorii rażącego niedbalstwa. Mogłoby to być co najwyżej niedbalstwo, czyli działanie o zwykłym stopniu winy, ale nie o stopniu kwalifikowanym-rażącym, a tylko taki w świetle art. 46 ust. 3 ustawy, zwalniałby pozwanego od odpowiedzialności w tej sprawie. Zdaniem Sądu powodowi nie można przypisać umożliwienia dokonania nieautoryzowanych transakcji wskutek rażącego niedbalstwa. Powód mógł pozostawać w przekonaniu, że aplikacja na stronie internetowej o tożsamej szacie graficznej co pozwanego Banku pochodzi właśnie od Banku, a żądanie instalacji programu antywirusowego jest procedurą konieczną do obsługi konta w telefonie komórkowym. Odpowiedzialność Banku za taką transakcję jest uchylona w razie doprowadzenia do nieautoryzowanej transakcji przez klienta w sposób umyślny lub wskutek umyślnego albo stanowiącego rażące niedbalstwo naruszenia obowiązków, o których mowa w art. 42.”*⁷

III. Przepisy UUP

⁷ Wyrok Sądu Okręgowego w Warszawie z dnia 20 kwietnia 2016 r., XXVII Ca 591/16, LEX nr 2574705.

Podstawę prawną dla kluczowych rozważań w obszarze pozwalającym na udzielenie odpowiedzi na postawione w początkowej części niniejszego poglądu pytania stanowić będą przede wszystkim przepisy art. 42 oraz art. 46 UUP, czyli regulacje dotyczące ewentualnych reperkusji dokonania transakcji nieautoryzowanej i związane z rozkładem ciężaru dowodu faktu autoryzacji transakcji płatniczej. W sytuacji wystąpienia nieautoryzowanej transakcji płatniczej ustalenie, który z podmiotów obciążają negatywne jej skutki, zależne jest od wielu okoliczności, takich jak np. to, czy doszło do naruszenia przez płatnika obowiązków ostrożnościowych nałożonych na niego w związku z korzystaniem z instrumentu płatniczego czy stopień winy płatnika. Nie może się zatem ostać twierdzenie pozwanego, iż konsekwencje opisanych w odpowiedzi na pozew przypadków obciążają klienta, nie zaś bank. Treść art. 46 UUP jasno wskazuje, że nawet niedbałe, czy niestaranne zachowania użytkownika, mogą obciążać bank w tym sensie, iż obowiązany będzie niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. Wynika to z pro-klienckiego charakteru omawianych przepisów. Pełna odpowiedzialność płatnika następuje tylko i wyłącznie wówczas, gdy doprowadził on do nieautoryzowanej transakcji nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 UUP.

Raz jeszcze należy podkreślić, że dokładnie z tego samego powodu nie jest prawidłowe twierdzenie pozwanego, iż art. 46 ust. 1 UUP wprowadza generalną zasadę odpowiedzialności, która jednak nie znajduje zastosowania do okoliczności, gdy sporna transakcja została spowodowana przez posiadacza rachunku. Wykładnia całego art. 46 UUP prowadzi do odmiennego wniosku, a mianowicie nawet przyczynienie się użytkownika do tego, iż doszło do nieautoryzowanej transakcji, nie będzie powodować jego pełnej odpowiedzialności, jeżeli nie było umyślne lub też jeżeli nie było skutkiem umyślnego lub rażąco niedbałego naruszenia obowiązków wynikających z art. 42 UUP.

Wymaga podkreślenia, iż za transakcję autoryzowaną uważa się wyłącznie taką transakcję płatniczą, na której przeprowadzenie płatnik (czyli w tym wypadku powódka) wyraził zgodę (art. 40 UUP). Udzielenie zgody (w uzgodniony między stronami sposób,

w okolicznościach przedmiotowej sprawy kwestia ta została uregulowana w regulaminie) **przez płatnika** jest zatem jedyną przesłanką autoryzacji danej transakcji płatniczej. Dopiero w takim wypadku można mówić o prawidłowo dokonanej transakcji płatniczej, np. za pomocą jednego z instrumentów płatniczych, jakim jest polecenie przelewu, dokonane za pomocą zlecenia płatniczego w systemie bankowości elektronicznej. Uprawnienie dostawcy (pozwanego) do przeprowadzenia transakcji płatniczej wynika zatem bezpośrednio z autoryzowania transakcji przez płatnika, czyli złożonego przez niego stosownego oświadczenia woli. Jeżeli zgoda na transakcję płatniczą nie została udzielona przez podmiot do tego uprawniony (np. posiadacza rachunku – powódkę), a dostawca wykonuje transakcję, to w ocenie Rzecznika Finansowego nie zyskuje on np. uprawnienia do obciążenia rachunku płatniczego płatnika ani do żądania od płatnika zwrotu kwoty, którą przekazał dostawcy usług płatniczych odbiorcy.

Wydaje się, że już na tym, etapie (a jednocześnie kluczowym dla ustalenia podmiotu odpowiedzialnego za dokonanie transakcji nieautoryzowanej) dokonywania transakcji płatniczej, pojawiają się istotne zagadnienia w kontekście sprawy powódki.

Należy zatem odpowiedzieć na pytanie, czy w sytuacji, w której transakcja dokonywana jest na podstawie działań podjętych przez inne niż płatnik (powódka) osoby – np. gdy dane uwierzytelniające uzyskane zostały przez osoby nieuprawnione w wyniku podejmowanych przez nie działań o charakterze przestępczym (a właśnie taka sytuacja, zdaniem powódki, miała miejsce w przedmiotowej sprawie) – co prowadzi do inicjacji transakcji płatniczej przez osoby trzecie wbrew woli (lub bez wiedzy) płatnika przy użyciu instrumentu płatniczego, którego płatnik jest posiadaczem, w ogóle można mówić o zgodzie płatnika na jej przeprowadzenie w rozumieniu art. 40 UUP. W okolicznościach powiązanych z atakiem *phishingowym*, tak jak miało to miejsce w przypadku powódki, trudno mówić o wyrażeniu zgody (dokonaniu wiążącego prawnie oświadczenia woli) na dokonanie transakcji płatniczej. Przyjmując pogląd, że w takim wypadku nie mamy do czynienia z wyrażeniem zgody w rozumieniu art. 40 ust. 1 UUP, konsekwentnie transakcję płatniczą należy uznać za nieautoryzowaną ze wszelkimi konsekwencjami z tego wynikającymi (w tym w szczególności z konsekwencjami wynikającymi art. 46 ust. 1 UUP), o czym będzie mowa niżej. Ustawodawca wprost wskazał w art. 40 ust. 1, że transakcję płatniczą uważa się za

autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Biorąc powyższe okoliczności faktyczne, bezspornym jest w ocenie obu stron postępowania, że to nie płatnik (powódka) wyraził zgodę na wykonanie spornej transakcji płatniczej.

W ocenie Rzecznika Finansowego należy przyjąć, że wyłudzenie od powódki danych uwierzytelniających czy podanie przez powódkę kodu BLIK w sytuacji dokonania oszukańczych działań nie stanowi automatycznie wyrażenia zgody w rozumieniu art. 40 ust. 1 UUP na dokonanie transakcji płatniczej – nie jest bowiem skutecznym oświadczeniem woli.

W tym kontekście warto raz jeszcze przytoczyć treść prawomocnego wyroku Sądu Okręgowego w Łodzi z dnia 11 stycznia 2017 r., sygn. III Ca 1401/16, w którym sąd na tle omawianej problematyki stwierdził, że: „*Stosownie do art. 40 ust 1 ustawy transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zgoda ta stanowi przy tym oświadczenie woli w rozumieniu art. 60 k.c. Jednocześnie przepis ten stanowi implementację art. 54 dyrektywy Nr 2007/64/WE, który mówi o tym, że państwa członkowskie zapewniają, aby transakcję płatniczą uważano za autoryzowaną tylko pod warunkiem udzielenia przez płatnika zgody na wykonanie transakcji płatniczej. (...) Co istotne, udzielenie zgody przez posiadacza jest w istocie jedyną przesłanką autoryzacji danej transakcji płatniczej (M. B. „Autoryzacja transakcji płatniczych i odpowiedzialność za transakcje nieautoryzowane”, opubl. „Prawo Bankowe” Nr 7-8/2012, s. 85 i n.)*”. W konsekwencji sąd uznał, że: „*Po jej stronie [po stronie powódki – przypomina Rzecznik Finansowy] nie wystąpiły bowiem żadne uchybienia ani wadliwości, za czym przemawia też jej szybka reakcja, sprowadzająca się do niezwłocznego powiadomienia banku i policji o „wyczyszczeniu” jej konta, co miało miejsce dnia 19 grudnia 2013 r., kiedy to powódka w historii rachunku zauważyła przelewy, których sama nie dokonywała. Tym samym racja leży po stronie Sądu Rejonowego, który prawidłowo ocenił, iż transakcje dokonane z konta powódki nie były przez nią autoryzowane*”.

Nie ma przy tym znaczenia z punktu widzenia ustalania odpowiedzialności pozwanego banku jako dostawcy usług płatniczych płatnika (powódki) prowadzącego rachunek płatniczy (bankowy), że nie doszło do złamania zabezpieczeń informatycznych systemu bankowego i np.

Str 12

nigdy nie odnotowano przypadku incydentu operacyjnego w postaci naruszenia posiadanych przez Bank zabezpieczeń. Art. 40 ust. 1 UUP oraz pozostałe artykuły regulujące przedmiotową materię nie uzależniają odpowiedzialności dostawcy usług płatniczych od wystąpienia takich okoliczności. Pozostają one zatem irrelevantne dla oceny prawnej przedmiotowej sprawy i ustalenia podmiotu ponoszącego odpowiedzialność za dokonanie nieautoryzowanej transakcji z rachunku powódki (oczywiście miałyby znaczenie, w sytuacji, gdyby zabezpieczenia banku istotnie zostały przełamane – wówczas można by rozpatrywać odpowiedzialność kontraktową banku). Należy jednak przy tej okazji podkreślić, że zapewnienie bezpieczeństwa depozytów jest jednym z najistotniejszych obowiązków banku, a sposób jego wykonywania jest najbardziej wymierną podstawą oceny jego wiarygodności, w związku z czym wszelkie próby interpretacji przez banki postanowień zawartych w stosowanych przez nie wzorcach umownych, zmierzające do zaniżania standardów bezpieczeństwa powierzonych bankowi środków pieniężnych, powinny być oceniane jako zachowania sprzeczne z dobrymi obyczajami i celem umowy rachunku bankowego (tak SN w wyr. z 14.04.2003 I CKN 308/61).

W ocenie Rzecznika Finansowego warto w trakcie postępowania ponadto wyjaśnić, czy pozwany Bank stosuje oprogramowanie, które bada statystykę operacji na rachunku klienta oraz tzw. oprogramowanie antyfraudowe, które bada anormalne działania na kontach klientów. Pozwoli to ustalić, czy pozwany w pełni zabezpieczał interesy klientów w chwili dokonywania ataków hakerskich przez osoby nieuprawnione.

W kontekście przedmiotowego aspektu niniejszej sprawy należy również wyjaśnić, czy pozwany bank posiada np. w regulacjach wewnętrznych tego podmiotu zasady bezpieczeństwa, o których szczegółowo informowano na stronie internetowej lub przez kanał dostępu telefonicznego klientów, np. ostrzegające przed *phishingiem*. Oczywiście nie zwalnia to Banku z odpowiedzialności, gdyż – jeśli takie zasady istniały – należy postawić pytanie o ich charakter prawny w kontekście stosunku zobowiązaniowego (umów i regulaminów) łączącej strony. W ocenie Rzecznika Finansowego jedynie umowom oraz regulaminowi można przypisywać jakąkolwiek moc prawną w sytuacjach spornych, bowiem samo bliżej nieokreślone „przekazanie” czy „poinformowanie” o tychże zasadach bezpieczeństwa powódki nie oznacza, że nastąpiło skuteczne – zgodnie z prawem zobowiązań – związanie

drugiej strony prawami i obowiązkami z takiego dokumentu wynikającymi. Nie bardzo zatem wiadomo, w jaki sposób należy kwalifikować ww. zasady bezpieczeństwa.

W takiej sytuacji należy uznać, że w sytuacjach spornych wyłącznie umowa oraz regulamin i wyrażone w treści tych dokumentów postanowienia mogą stanowić podstawę prawną do formułowania ewentualnych roszczeń oraz wniosków w odniesieniu do ich przestrzegania przez obie strony stosunku zobowiązaniowego.

Przykładowo na tle sporu wynikającego z umowy kredytu, Sąd Najwyższy w wyroku z dnia 7.05.2004 r., I CK 686/03 (PB 2005 nr 6, str. 9) stwierdził, że: „Regulacje zawarte w instrukcjach służbowych przeznaczonych dla pracowników pozwanego banku mają jedynie charakter zarządzeń wewnętrznych. Tym samym nie mogą stanowić dyrektywy interpretacyjnej zmierzającej do uzupełnienia treści zawartej przez strony umowy kredytu”. Należy zatem przyjąć, że zarówno wewnętrzne regulacje (zarządzenia) proferenta, jak i wszelkiego rodzaju instrukcje służbowe pozostają bez znaczenia dla treści umowy i obowiązków powódki.

Fakt, że powódka generalnie pozostaje wierzycielem Banku na mocy art. 725 k.c. i nast., nie ma znaczenia z punktu widzenia rozkładu odpowiedzialności z tytułu dokonania nieautoryzowanych transakcji płatniczych, pozostających w reżimie UUP. W tym kontekście należy wskazać, że zobowiązanie Banku względem posiadacza rachunku kształtuje również art. 50 ust. 2 ustawy prawo bankowe, który stanowi, iż bank jest zobowiązany do dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych.

Niezależnie od powyższego, bliższej analizy wymagają również pozostałe regulacje szczegółowe, kształtujące rozkład odpowiedzialności podmiotów uczestniczących w dokonaniu transakcji płatniczej. Dyrektywa PSD2, a w ślad za nią polski ustawodawca, zdecydował o ustanowieniu generalnej zasady, zgodnie z którą ryzyko odpowiedzialności z tytułu przeprowadzenia nieautoryzowanej transakcji płatniczej spoczywa w całości na dostawcy usług płatniczych – w tym wypadku na Banku (art. 46 ust. 1 w zw. z art. 45 ust. 1 i 2 UUP). Warto wskazać, że wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana (art. 45 ust. 2 UUP). Fakt skutecznego zainicjowania

transakcji płatniczej za pomocą polecenia przelewu poprzez system bankowości elektronicznej nie jest zatem wystarczający do uznania, że uprawniony użytkownik dokonał autoryzacji.

Konsekwentnie, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej zastosowanie znajdzie art. 46 ust. 1 UPP, zgodnie z którym, *„Z zastrzeżeniem art. 44 ust. 2, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza”*. Jest to więc ogólna reguła, nakładająca na dostawcę (w przedmiotowej sprawie na Bank), konkretny obowiązek, z którego Bank powinien się wywiązać. Co istotne, mimo tego, iż w konkretnie wskazanych w ustawie okolicznościach odpowiedzialność za nieautoryzowaną transakcję ponosi płatnik (art. 46 ust. 2 i 3 UUP), to żaden przepis UUP nie uchyla obowiązku wynikającego z art. 46 ust. 1 UUP. Jedyne wyjątek w tym zakresie stanowi art. 44 ust. 2 UUP, jednak sytuacja ta nie ma miejsca w przedmiotowej sprawie.

I tak, zgodnie z art. 46 ust. 2 UUP, *„Płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 50 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji, jeżeli nieautoryzowana transakcja jest skutkiem:*

- 1) posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub*
- 2) przywłaszczenia instrumentu płatniczego”.*

Z kolei, zgodnie z ust. 3 tego artykułu, *„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”*.

Dostawca jest zatem obowiązany udowodnić inne okoliczności, wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej lub wskutek rażącego

niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 UUP. Ustawodawca, w celu zagwarantowania bezpieczeństwa i pewności obrotu bezgotówkowego, zdecydował się zatem na odwrócenie zasady ciężaru dowodu z art. 6 k.c. i art. 232 k.p.c. UUP wskazuje, w jakich sytuacjach możliwym jest zwolnienie się przez dostawcę od ponoszenia ww. odpowiedzialności.

Wreszcie, art. 46 ust. 3 UUP stanowi, że płatnik będzie odpowiadał za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nieautoryzowanych transakcji umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków wskazanych w art. 42 UUP. Z kolei, na mocy art. 42 ust. 2 UUP na płatnika nałożono obowiązek podejmowania niezbędnych środków służących zapobieżeniu naruszeniu indywidualnych zabezpieczeń instrumentu płatniczego, w tym przechowywaniu instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym. Należy zatem odpowiedzieć na pytanie, czy w podobnych do przedmiotowej sprawy okolicznościach, zasadnym jest przyjęcie (tak jak zrobił to Bank), że użytkownik – który padł ofiarą oszustwa (poprzez zastosowanie wobec niego podstępu) oraz kradzieży – naruszył ww. obowiązek w wyniku rażąco niedbałego zachowania. Sytuacja byłaby prawdopodobnie prostsza (choć wcale nie jednoznaczna) w przypadku, gdyby osoba np. otrzymała prośbę przesłaną drogą elektroniczną (w postaci np. standardowej wiadomości e-mail, niewskazującej na jakikolwiek związek z Bankiem) od nieznanego nadawcy o udostępnienie danych autoryzujących oraz uwierzytelniających w celu wykorzystania ich w dowolnym celu (choćby np. sprawdzenia, czy dostęp do bankowości elektronicznej nie został zablokowany) i prośba ta została przez użytkownika spełniona. Tymczasem, często w podobnych okolicznościach do sprawy powódki, możemy mieć jednak do czynienia ze świetnie przygotowanym atakiem *phishingowym*. W ocenie Rzecznika, trudno jest zatem przyjąć interpretację, zgodnie z którą zachowanie płatnika-użytkownika danego instrumentu płatniczego polegające na nieświadomym udostępnieniu danych osobom nieuprawnionym, w starciu z „profesjonalistami” i zastosowanymi przez nich metodami oszukańczymi, należy automatycznie ocenić jako rażące niedbalstwo. Kwestia ta wymaga udowodnienia, jednakże ciężar dowodu spoczywa na dostawcy (Banku) i przeprowadzenie dowodów w tym zakresie może nastąpić tylko i wyłącznie w postępowaniu sądowym. Zresztą, należy w tym miejscu jeszcze raz podkreślić, o czym była mowa wyżej, że

Str. 16

samo nawet rażąco niedbałe zachowanie płatnika nie jest wystarczające dla uznania jego odpowiedzialności, konieczne jest bowiem naruszenie – umyślnie lub w wyniku rażącego niedbalstwa – przez płatnika co najmniej jednego z obowiązków, o których mowa w art. 42 UUP (art. 46 ust. 3 UUP). Wydaje się, że w tym zakresie okoliczności również nie zostały udowodnione.

Tytułem uzupełnienia powyższych rozważań należy także *explicite* podkreślić, że w art. 45 ust. 2 UUP ustawodawca nakłada na dostawcę ciężar dowodu również w zakresie będącego skutkiem rażącego niedbalstwa naruszenia przez użytkownika obowiązków wskazanych w art. 42 UUP. Oznacza to, że dostawca zobowiązany jest do udowodnienia, że użytkownik wykazał się rażącym niedbalstwem w naruszeniu obowiązków, o których mowa w art. 42 UUP i doprowadził w jego wyniku do wystąpienia nieautoryzowanej transakcji płatniczej, szczególnie w sytuacji, w której zaprzecza on zaistnieniu takich okoliczności (tak jak ma to miejsce w przypadku powódki). Należy zatem dodatkowo odróżnić sytuację, w której użytkownik sam przyznaje się do podania przedmiotowych danych autoryzujących i uwierzytelniających osobom nieuprawnionym. Nie oznacza to jednak automatycznie, że transakcja została autoryzowana ani też nie należy automatycznie przyjmować interpretacji o kwalifikowanej winie (rażącym niedbalstwie) danego użytkownika. W ocenie Rzecznika, kwestia ta każdorazowo powinna być oceniana przez pryzmat wszystkich okoliczności zaistniałych w sprawie z uwzględnieniem poczynionych wyżej rozważań.

Powyższe rozważania potwierdza orzecznictwo sądów powszechnych, np. w wyr. z dnia 15.01.2016 r. Sądu Okręgowego w Łodzi (sygn. akt. I C 307/15), w wyr. z dnia 8.02.2016 r. tego samego sądu (sygn. I C 1908/14), wyr. Sądu Okręgowego w Łodzi z dnia 11.01.2017 r., sygn. III Ca 1401/16, czy wyr. Sądu Okręgowego w Łodzi z 20.03.2017 r., sygn. III Ca 1753/16.

W opinii Rzecznika Finansowego zatem w okolicznościach niniejszej sprawy trudno mówić o możliwości przypisania pełnej odpowiedzialności za dokonanie nieautoryzowanej transakcji powódce. Należy także pamiętać, że zgodnie z art. 45 ust. 1 UUP, ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Wydaje się też, że zachowanie Powódki nie graniczyło z umyślnością, a więc nie miało cech rażącego

niedbalstwa. Z kolei zgodnie z art. 45 ust. 2 UUP: „Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana. 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 lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42”.

Tytułem zakończenia Rzecznik Finansowy pragnie oddać także pod rozwagę tut. Sądu niezwykle istotny z punktu widzenia rozpatrywanej sprawy wyrok Sądu Najwyższego z dnia 18 stycznia 2018 r. o sygn. V CSK 141/17. Stanowi on ugruntowanie dotychczasowej linii orzeczniczej w sprawach dotyczących nieautoryzowanych transakcji płatniczych. SN potwierdził w nim m.in., że *Zarzut naruszenia art. 45 ust. 2 u.o.u.p. w związku z art. 6 k.c. dotyczy niewłaściwego ich zastosowania i przyjęcia, że pozwany nie udowodnił, aby powódka dopuściła się rażącego niedbalstwa przy wykonywaniu umowy o świadczenie usług bankowości internetowej. Zgodnie z art. 45 ust. 1 u.o.u.p., w drodze wyjątku od zasady określonej w art. 6 k.c., ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Według art. 45 ust. 2 u.o.u.p, wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana. 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 lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42. Jak już wspomniano, w niniejszej sprawie w ogóle nie ma mowy o naruszeniu przez powódkę obowiązków określonych w art. 42 u.o.u.p. Poza tym Bank oczywiście nie wykazał, że powódka umyślnie doprowadziła do nieautoryzowanej transakcji płatniczej.*

IV. Wniosek końcowy

Rzecznik Finansowy, po przanalizowaniu stanowiska stron, wskazuje, że w jego ocenie

Str. 18

istnieje wysokie prawdopodobieństwo wystąpienia okoliczności faktycznych, wskazywanych przez Powódkę w powództwie.

Przedstawiając powyższe stanowisko, Rzecznik Finansowy wyraża nadzieję, że okaże się ono pomocne dla wydania rozstrzygnięcia w niniejszej sprawie.

Jednocześnie z uwagi na prowadzone przez nas analizy orzecznictwa, zwracam się z uprzejmą prośbą o poinformowanie Rzecznika Finansowego o wynikach postępowania sądowego, przesyłając kopię orzeczenia sądu.

Załączniki:

1. kopia wniosku o wydanie istotnego poglądu w sprawie wraz z kopią pełnomocnictwa;
2. kopia pełnomocnictwa upoważniającego do składania oświadczeń zawierających pogląd istotny dla sprawy w imieniu Rzecznika Finansowego;
3. dwa odpisy oświadczenia Rzecznika Finansowego zawierające pogląd istotny dla sprawy.

