NIEAUTORYZOWANE TRANSAKCJE – ZASADY I GŁÓWNE PROBLEMY

1. Wstęp

Każdego dnia roboczego do Rzecznika Finansowego trafia przynajmniej jeden oficjalny wniosek o wszczęcie postępowania interwencyjnego w sprawie nieautoryzowanej transakcji płatniczej. Niemal równie częste są zapytania telefoniczne lub e-mailowe o sposób radzenia sobie z tym problemem. Sprawy trafiające do Rzecznika Finansowego można podzielić na trzy główne kategorie. Dotyczą one: rachunków bankowych, kart debetowych i kart kredytowych.

W niniejszym opracowaniu skoncentrujemy się na tej pierwszej kategorii, ponieważ skargi związane z rachunkami bankowymi są najliczniejsze. Warto jednak podkreślić, że zasady odpowiedzialności tzw. dostawcy usługi płatniczej (czyli najczęściej banku lub operatora karty), określone w dyrektywie PSD II[1], a wdrożone do polskiego prawodawstwa ustawą o usługach płatniczych[2], są takie same bez względu na to, jakiego instrumentu dotyczy nieautoryzowana transakcja.

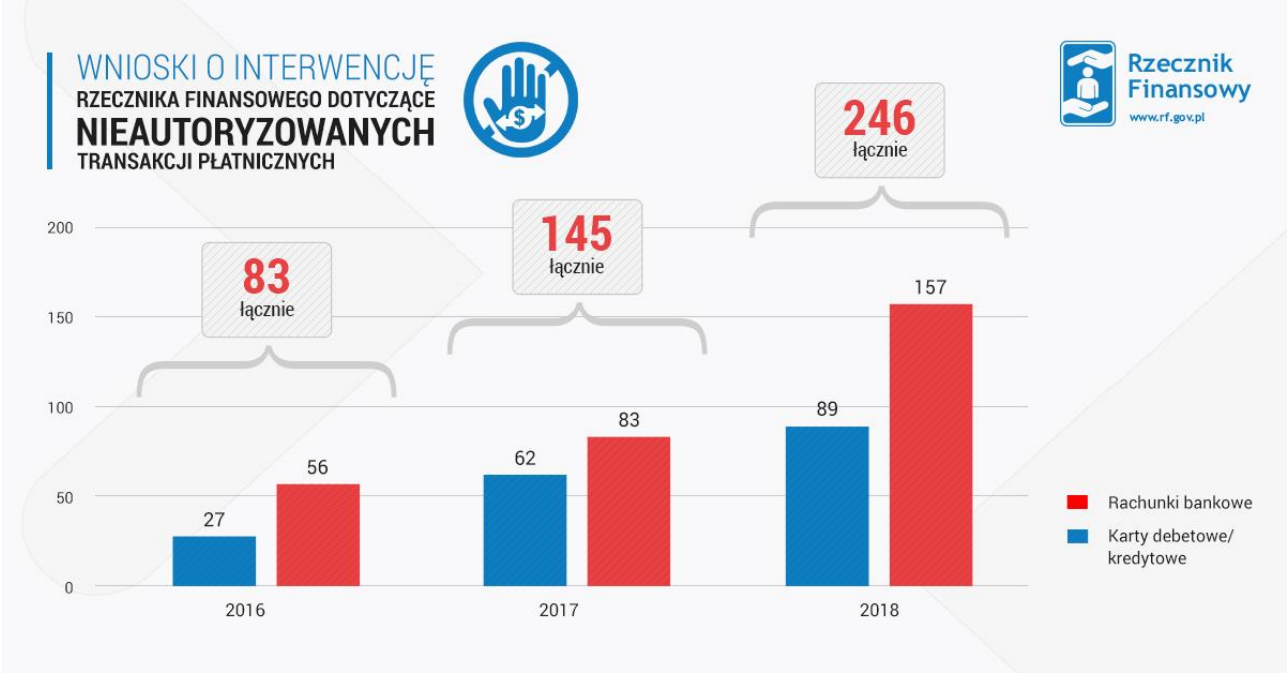
Niestety, Rzecznik Finansowy dostrzega w obszarze nieautoryzowanych transakcji płatniczych – w szczególności w zakresie postępowania dostawców, głownie banków – dwa niepokojące trendy, które to stały się bezpośrednią przyczyną przygotowania niniejszej Analizy.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337/35 z dnia 23 grudnia 2015 r. z późn. zm., dalej: dyrektywa PSD II).

[2] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2019 r. poz. 659 z późn. zm., dalej: u.u.p. lub ustawa o usługach płatniczych).

Po pierwsze, rośnie liczba wniosków o przeprowadzenie tzw. postępowania interwencyjnego Rzecznika Finansowego w związku z nieautoryzowaną transakcją płatniczą. W 2018 r. było ich 246, podczas gdy rok wcześniej – 145. Warto też podkreślić, że Rzecznik notuje dynamiczny wzrost liczby takich spraw. Dla porównania tylko w I kwartale 2019 r. pojawiły się 83 takie wnioski, czyli dokładnie tyle samo co w całym 2016 r.

Poniżej graficzne przedstawienie problemu narastania liczby skarg.



Część klientów, zanim złoży oficjalny wniosek o interwencję, zwraca się do ekspertów Rzecznika Finansowego z prośbą o poradę udzielaną drogą telefoniczną lub e-mailową. W 2018 r. eksperci Rzecznika Finansowego odebrali łącznie 214 telefonów oraz e-maili dotyczących nieautoryzowanych transakcji płatniczych na rachunkach bankowych i kartach (odpowiednio 110 i 104 prośby o poradę).

Po drugie, Rzecznik Finansowy zaobserwował, że trafiające do niego skargi dotyczą sytuacji, w której klient po zgłoszeniu nieautoryzowanego przelewu nie otrzymał niezwłocznie zwrotu utraconych środków. Tymczasem wspomniana dyrektywa PSD II oraz ustawa o usługach płatniczych wprowadzają tzw. zasadę D+1. Zgodnie z nią taki zwrot powinien trafić na konto klienta niezwłoczne, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji. Gdyby ta zasada była przestrzegana przez banki, ewentualne wnioski o wsparcie trafiałby do Rzecznika Finansowego dopiero na etapie skierowania przez bank do klienta żądania zwrotu środków. Obecnie klienci proszą o pomoc w odzyskaniu pieniędzy utraconych w wyniku nieautoryzowanej transakcji. Z opisów skarg trafiających do Rzecznika Finansowego wynika, że obowiązki nałożone na dostawców przez dyrektywę PSD II i

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

ustawę o usługach płatniczych nie tylko nie są realizowane w przepisowym terminie, ale wręcz klienci oczekują na zwrot przez wiele tygodni, a nawet miesięcy – i wówczas szukają wsparcia Rzecznika Finansowego. Oznacza to, że klient nie otrzymuje zwrotu kwoty po zgłoszeniu nieautoryzowanej transakcji, nie pomaga też złożenie reklamacji. Niestety, trzeba zaznaczyć, że nawet znaczna część działań Rzecznika Finansowego w ramach postępowania interwencyjnego nie przynosi efektów w postaci zmiany postępowania dostawców. Z danych Rzecznika Finansowego dotyczących wniosków zgłoszonych po wejściu w życie obecnie obowiązujących uregulowań (czyli po dniu 20 czerwca 2018 r.), wynika, że około 40% sporów dotyczących transakcji na rachunkach bankowych zakończyło się zmianą stanowiska banku dopiero w wyniku interwencji Rzecznika Finansowego. Warto jednak podkreślić, że statystyki te mogą ulec zmianie, gdyż nadal około 75% spraw zgłoszonych w tym okresie jest w toku ze względu na długotrwałą wymianę pism z bankami. W tego typu sprawach Rzecznik Finansowy często wymienia 2–3 pisma, starając się argumentacją prawną przekonać dany bank do zmiany stanowiska.

Rzecznik Finansowy obserwuje też przypadki, w których ofiara oszustwa nie tylko traci pieniądze zgromadzone na koncie, ale też w jej imieniu zaciągany jest kredyt (więcej w opisie przypadku w rozdziale *Z akt Rzecznika Finansowego*). Dodatkowo w takich sytuacjach część banków nie wstrzymuje się z żądaniem spłaty kolejnych rat kredytu, przynajmniej do czasu wyjaśnienia sprawy. Niestety, uproszczona procedura przyznania kredytu (nazywana często marketingowo „na klik") powoduje, że przestępcy po przejęciu kontroli nad dostępem do konta ofiary wykorzystują wszelkie dostępne możliwości pozyskania finasowania. Stąd apel Rzecznika Finansowego do banków o wprowadzenie dodatkowych zabezpieczeń, które uniemożliwiłyby taki proceder.

Należy się spodziewać, że w najbliższych latach problem będzie narastał. Ma to związek z dynamicznym rozwojem technologicznym rynku usług płatniczych w obszarze płatności elektronicznych, w szczególności w zakresie bankowości mobilnej (ang. *m-banking*), bankowości elektronicznej (ang. *e-banking*), otwartej bankowości (ang. *open banking*) czy płatności kartami. Również pojawienie się nowych rodzajów usług płatniczych będzie się przekładać na wzrost liczby płatności elektronicznych.

Także usługi *e-commerce* stają się coraz bardziej popularne wśród konsumentów, którzy częściej i chętniej dokonują zakupów przez internet, opłacając je z wykorzystaniem płatności elektronicznych. Wszystko to sprawia, że liczba prób kradzieży i wyłudzeń z wykorzystaniem transakcji płatniczych oraz elektronicznych i mobilnych kanałów dostępu do tych usług stale rośnie.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

Jak wynika z raportu CERT Polska[3] za 2018 r.[4] przypadki tzw. phishingu (który prowadzi do nieautoryzowanej transakcji) wyróżniają się na tle pozostałych ataków. W 2018 r. zarejestrowano 1655 takich incydentów, co stanowiło 44% z ogółu naruszeń bezpieczeństwa w sieci. Jak napisano w raporcie CERT: „Scenariusze dotyczące podszywania się pod pośredników płatności, stały się w 2018 roku najpopularniejszym atakiem na użytkowników bankowości elektronicznej, powodując znaczne straty finansowe. W 2018 roku scenariusz zaczął być wykorzystywany w klasycznych fałszywych sklepach, szczególnie w końcowej »fazie życia« takiego sklepu. Rośnie liczba złośliwych aplikacji dla urządzeń mobilnych, przede wszystkim z systemem Android. Wiele z nich, między innymi podszywających się pod legalne aplikacje finansowe, dostępnych było do pobrania w oficjalnym sklepie".

Mając na uwadze ochronę klientów podmiotów rynku finansowego w kontekście wskazanej powyżej problematyki oraz stanowisko dostawców usług płatniczych, Rzecznik Finansowy dokonał analizy prawnej zmian, jakie zaszły w systemie prawnym, w zakresie sposobu postępowania dostawców usług płatniczych w przypadku wystąpienia nieautoryzowanej transakcji płatniczej.

Celem tego opracowania jest również podsumowanie obserwacji Rzecznika Finansowego odnoszących się do podejścia dostawców do sposobu rozpatrywania reklamacji dotyczących nieautoryzowanych usług płatniczych oraz przedstawienie stanowiska Rzecznika Finansowego w tej kwestii.

[3] Zespół CERT Polska to zespół reagowania na incydenty (z ang. *Computer Emergency Response Team*). Działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – państwowego instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne.

[4] https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa

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

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

2. Nieautoryzowane transakcje – stan prawny

W dniu 20 czerwca 2018 r. weszły w życie przepisy ustawy z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw[5], stanowiące implementację dyrektywy PSD II. Wprowadzone zmiany do ustawy o usługach płatniczych dotyczą między innymi zasad odpowiedzialności płatnika oraz sposobu postępowania dostawcy w przypadku wystąpienia nieautoryzowanej transakcji płatniczej. Celami dyrektywy PSD II – poza dostosowaniem przepisów do zachodzących na rynku zmian oraz ustandaryzowaniem przepisów regulujących rynek płatności – są także zapewnienie konsumentom większego bezpieczeństwa i zwiększenie zakresu ich ochrony.

a) Czym jest nieautoryzowana transakcja płatnicza?

Ustawa o usługach płatniczych nie zawiera definicji legalnej pojęcia nieautoryzowanej transakcji płatniczej. Zgodnie natomiast z art. 40 ust. 1 u.u.p. 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 może dotyczyć także kolejnych transakcji płatniczych.

> **Można zatem uznać, że z nieautoryzowaną transakcją płatniczą mamy do czynienia w sytuacji, gdy płatnik nie wyraził na nią zgody.**

Udzielenie zgody przez płatnika w uzgodniony między stronami sposób jest jedyną przesłanką autoryzacji danej transakcji płatniczej. Dopiero w takim wypadku można mówić o prawidłowo dokonanej transakcji płatniczej. Uprawnienie dostawcy do przeprowadzenia transakcji płatniczej wynika zatem bezpośrednio z autoryzowania transakcji przez płatnika. Jeżeli zgoda na transakcję płatniczą nie została udzielona przez podmiot do tego uprawniony (np. przez posiadacza rachunku), a dostawca wykonuje transakcję, to w ocenie Rzecznika Finansowego nie zyskuje on uprawnienia ani do obciążenia rachunku płatniczego płatnika, ani do żądania od płatnika zwrotu kwoty, którą przekazał dostawcy usług płatniczych odbiorcy.

Analizując tę kwestię w kontekście coraz bardziej powszechnych i wyrafinowanych przestępstw wyłudzenia danych autoryzacyjnych płatników, np. przy użyciu metod phishingowych, należy zadać pytanie: Czy w sytuacji, w której transakcja płatnicza dokonywana jest na podstawie działań podjętych przez inne niż płatnik osoby (osoby trzecie), wbrew woli i świadomości płatnika, w wyniku podejmowanych przez nie

[5] Dz. U. poz. 1075.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 26
22 333 73 27
fax. 22 333 73 29

działań o charakterze przestępczym, w ogóle można mówić o świadomej zgodzie płatnika na jej przeprowadzenie w rozumieniu art. 40 u.u.p.?

> **Wydaje się, że w okolicznościach powiązanych z atakiem phishingowym lub jakimkolwiek innym działaniem przestępczym trudno mówić o skutecznym wyrażeniu zgody na dokonanie transakcji płatniczej.**

Przyjmując pogląd, że w takim wypadku nie mamy do czynienia z wyrażeniem zgody w rozumieniu art. 40 ust. 1 u.u.p., konsekwentnie transakcje płatniczą należy uznać za nieautoryzowaną – ze wszelkimi skutkami z tego wynikającymi, w szczególności z obowiązkami wynikającymi z art. 46 ust. 1 u.u.p.

Warto podkreślić, że polski ustawodawca – w ślad za dyrektywą PSD II – zdecydował o ustanowieniu generalnej zasady, zgodnie z którą **ryzyko odpowiedzialności z tytułu przeprowadzenia nieautoryzowanej transakcji płatniczej spoczywa w całości na dostawcy usług płatniczych** (art. 46 ust. 1 w zw. z art. 45 ust. 1 i 2 u.u.p.). 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 u.u.p.). Zatem fakt skutecznego zainicjowania transakcji płatniczej przez system bankowości elektronicznej nie jest zatem wystarczający do uznania, że autoryzacji dokonał uprawniony użytkownik.

b) Konsekwencje uznania transakcji płatniczej za nieautoryzowaną

W wyniku wdrożenia dyrektywy PSD II zmianie uległ art. 46 u.u.p. Do dnia 20 czerwca 2018 r. w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika był 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.

Zgodnie z nowym brzmieniem art. 46 ust. 1 u.u.p. 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

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

płatnika przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Zmiana ta w ocenie Rzecznika Finansowego ma kolosalne znaczenie dla procedury postępowania w razie wystąpienia nieautoryzowanej transakcji płatniczej. Zdaniem Rzecznika zgodnie z obecnym stanem prawnym w przypadku wystąpienia nieautoryzowanej transakcji można mówić o kilku podstawowych zasadach.

Zasada 1: obowiązek bezwarunkowego zwrotu środków klientowi

Z przepisu art. 46 ust. 1 u.u.p. po nowelizacji wynika przede wszystkim, że ustawodawca krajowy, w ślad za ustawodawcą unijnym, wprowadził obowiązek bezwarunkowego zwrotu kwoty nieautoryzowanej transakcji płatnikowi przez dostawcę, w przypadku zgłoszenia przez płatnika wystąpienia nieautoryzowanej transakcji lub stwierdzenia przez dostawcę tego faktu. Od zasady tej są dwa wyjątki, o czym będzie mowa w dalszej części niniejszej Analizy. Można zatem powiedzieć, że sam fakt zgłoszenia przez płatnika nieautoryzowanej transakcji – szczególnie w postaci reklamacji – lub wykrycie przez dostawcę nieautoryzowanej transakcji powodują, iż dostawca jest zobowiązany do zwrotu środków płatnikowi.

Zasada 2: obowiązek zwrotu kwoty nieautoryzowanej transakcji w terminie D+1

Dostawca powinien dokonać zwrotu kwoty nieautoryzowanej transakcji niezwłocznie, a najpóźniej następnego dnia roboczego po zgłoszeniu lub wykryciu nieautoryzowanej transakcji. Ustawodawca unijny postanowił wprowadzić zatem bardzo krótki termin dla dostawcy na zwrot kwoty nieautoryzowanej transakcji płatniczej, jednocześnie nakładając na niego obowiązek przyjęcia takich procedur wewnętrznych, które pozwolą mu na przeprowadzenie w rozsądnym terminie dochodzenia, czy nie doszło w danym przypadku do nieuczciwego działania samego użytkownika usług płatniczych. Ustalenie konkretnego dnia, w którym ma nastąpić zwrot środków, jest niezmiernie ważne w kontekście obliczania ewentualnych odsetek za zwłokę czy też przedawnienia roszczenia.

Zasada 3: ustalenie zasad ewentualnej odpowiedzialności płatnika za nieautoryzowaną transakcję dopiero po zwrocie środków

W ocenie Rzecznika Finansowego z uwagi na co do zasady bezwarunkowy obowiązek zwrotu środków nieautoryzowanej transakcji płatniczej przez dostawcę, zaraz po jej wykryciu lub stwierdzeniu, **dopiero po dokonaniu tego zwrotu następuje ustalenie zasad ewentualnej współodpowiedzialności płatnika za nieautoryzowaną transakcję płatniczą**. Ustalenie tej współodpowiedzialności związane jest z oceną faktyczną i prawną pewnych zdarzeń, stąd w ocenie Rzecznika Finansowego powinna ona następować w toku postępowania sądowego. W tym zakresie warto podsumować kilka reguł ustalenia współodpowiedzialności.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

Po pierwsze, po dokonaniu zgłoszenia – dostawcy lub podmiotowi wskazanemu przez dostawcę – utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu **płatnik nie odpowiada** za nieautoryzowane transakcje płatnicze, **chyba że doprowadził umyślnie do nieautoryzowanej transakcji**. Podobnie w przypadku gdy dostawca płatnika nie wymaga silnego uwierzytelniania użytkownika[6], płatnik nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że działał umyślnie. O ile udowodnienie faktu i daty zgłoszenia nieautoryzowanej transakcji czy też używania przez dostawcę silnego uwierzytelniania raczej nie powinny nastręczać trudności dostawcy, o tyle wykazanie umyślności jest już kwestią bardziej złożoną, wymagającą przeprowadzenia dowodu.

Po drugie, zgodnie z art. 46 ust. 2 u.u.p. do czasu zgłoszenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu **płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 50 euro**, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski i obowiązującego w dniu wykonania transakcji w przypadkach, gdy nieautoryzowana transakcja jest skutkiem posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub przywłaszczenia instrumentu płatniczego. **Płatnik nie odpowiada** za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 50 euro, jeżeli nie miał możliwości stwierdzenia utraty, kradzieży lub przywłaszczenia instrumentu płatniczego przed wykonaniem transakcji płatniczej – z wyjątkiem przypadku, gdy płatnik działał umyślnie lub utrata instrumentu płatniczego przed wykonaniem transakcji płatniczej została spowodowana działaniem lub zaniechaniem ze strony pracownika, agenta lub oddziału dostawcy płatnika albo podmiotu świadczącego na jego rzecz usługi (dostawców usług technicznych).

Po trzecie, zgodnie z art. 46 ust. 3 u.u.p. do czasu zgłoszenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu 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 u.u.p. Zgodnie z powoływanym przepisem płatnik obowiązany jest do

[6] Art. 2 pkt 26aa u.u.p.: „**silne uwierzytelnianie użytkownika** – uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:
a) wiedza o czymś, o czym wie wyłącznie użytkownik,
b) posiadanie czegoś, co posiada wyłącznie użytkownik,
c) cechy charakterystyczne użytkownika
– będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych”.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 26
22 333 73 27
fax. 22 333 73 29

korzystania z instrumentu płatniczego zgodnie z umową ramową oraz do podejmowania niezbędnych środków służących zapobieżeniu naruszeniu indywidualnych danych uwierzytelniających, w tym do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz do nieudostępniania go osobom nieuprawnionym. Obowiązany jest on również do zgłaszania niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. Wykazanie przez dostawcę umyślności w działaniu lub umyślnego albo będącego skutkiem rażącego niedbalstwa naruszenia obowiązków wynikających z art. 42 u.u.p. również wymaga w ocenie Rzecznika Finansowego przeprowadzenia dowodu i wykazania tych okoliczności przez dostawcę.

> **Dlatego też w ocenie Rzecznika Finansowego ustalenie zasad odpowiedzialności płatnika za nieautoryzowaną transakcję płatniczą powinno odbywać się w toku postępowania sądowego. Dostawca, zazwyczaj bank, powinien zatem pozwać klienta o zwrot kwoty transakcji, którą według jego oceny, powinien być obciążony płatnik.**

Nie bez znaczenia dla przyjęcia takich właśnie zasad postępowania w przypadku nieautoryzowanej transakcji płatniczej jest fakt **przerzucenia ciężaru dowodu większości istotnych okoliczności dotyczących ustalenia zasad odpowiedzialności płatnika na dostawcę**. Zgodnie bowiem z art. 45 ust. 1 u.u.p. na dostawcy użytkownika spoczywa ciężar udowodnienia, że transakcja płatnicza **została autoryzowana** i prawidłowo zapisana w systemie służącym do obsługi transakcji płatniczych dostawcy oraz że nie miała na nią wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą świadczoną przez tego dostawcę, w tym dostawcę świadczącego usługę inicjowania transakcji płatniczej. Analogicznie odpowiedzialność spoczywa na dostawcy inicjującym transakcję płatniczą. Usługa inicjowania płatności jest pewnym *novum* na rynku, które zapewne będzie zyskiwało na popularności, i oznacza usługę polegającą na zainicjowaniu zlecenia płatniczego na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego posiadanego u innego dostawcy usług płatniczych.

Dodatkowo zgodnie z art. 45 ust. 2 u.u.p. wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego, czyli użycia instrumentu płatniczego zgodnie z procedurami i przy zastosowaniu ustalonych w umowie z płatnikiem sposobów autoryzacji, nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana albo że płatnik umyślnie lub wskutek rażącego niedbalstwa 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 u.u.p. Ciężar udowodnienia tych okoliczności również spoczywa na dostawcy.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

Reasumując, w ocenie Rzecznika Finansowego, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej – z uwagi na obowiązek niezwłocznego zwrotu przez dostawcę kwoty nieautoryzowanej transakcji płatniczej – w pierwszej kolejności powinien nastąpić zwrot środków płatnikowi, a następnie – w wyniku ustalenia zakresu odpowiedzialności płatnika za nieautoryzowaną transakcję płatniczą – dostawca powinien wystąpić do płatnika z roszczeniem o zwrot całości lub części kwoty nieautoryzowanej transakcji płatniczej (w zależności od stopnia odpowiedzialności).

c) Wyjątki od zasady obowiązku bezwarunkowego zwrotu środków klientowi

Zdaniem Rzecznika Finansowego są tylko dwa wyjątki od zasady bezwarunkowego zwrotu środków klientowi. Po pierwsze, udokumentowane podejrzenie oszustwa i zawiadomienie organów ścigania. Po drugie, niedochowanie przez klienta terminu zgłoszenia nieautoryzowanej transakcji. Szczegółowe zasady zostaną omówione poniżej.

Udokumentowane podejrzenie oszustwa i zawiadomienie organów ścigania

Zgodnie z art. 46 ust. 1 u.u.p. dostawca po zgłoszeniu lub wykryciu nieautoryzowanej transakcji płatniczej może wstrzymać się z niezwłocznym zwrotem kwoty nieautoryzowanej transakcji płatniczej, w przypadku gdy ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw. Ze względu na obserwowaną przez Rzecznika Finansowego praktykę nieprawidłowego interpretowania tego przepisu przez niektórych dostawców, głównie banki, Rzecznik pragnie zwrócić uwagę na kluczowe znaczenie użytego w tym przepisie słowa „oszustwo". Dostawcy interpretują użyte w tym przepisie słowo „oszustwo" jako każde oszustwo, którego wynikiem jest nieautoryzowana transakcja płatnicza. Zatem za oszustwo w rozumieniu tego przepisu uznają również przykładowo kradzież środków z rachunku klienta w wyniku działania osób trzecich za pomocą na przykład phishingu. W ocenie Rzecznika Finansowego słowo „oszustwo" należy interpretować bardzo wąsko. I choć ustawa o usługach płatniczych, wdrażająca do naszego systemu prawnego przepisy dyrektywy PSD II, jasno nie precyzuje tej kwestii, Rzecznik Finansowy uważa, że odpowiedzi na pytanie, jakie oszustwo miał na myśli unijny ustawodawca, należy szukać w przepisach samej dyrektywy PSD II.

Warto więc sięgnąć, do motywu 71 dyrektywy, który stanowi jak poniżej [wyróżnienia autora].

> *„W przypadku nieautoryzowanej transakcji płatniczej dostawca usług płatniczych powinien bezzwłocznie zwrócić płatnikowi kwotę tej transakcji. Jeżeli jednak zachodzi duże prawdopodobieństwo nieautoryzowanej*

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 26
22 333 73 27
fax. 22 333 73 29

transakcji ***wynikającej z działania użytkownika usług płatniczych w nieuczciwych zamiarach****, a podejrzenie to opiera się na obiektywnych podstawach zgłoszonych odpowiedniemu organowi krajowemu, przed dokonaniem zwrotu na rzecz płatnika dostawca usług płatniczych powinien być w stanie przeprowadzić w rozsądnym terminie dochodzenie. Aby zapobiec wszelkim sytuacjom niekorzystnym dla płatnika, data waluty w odniesieniu do uznania rachunku kwotą zwrotu nie powinna być późniejsza niż data obciążenia rachunku tą kwotą. Aby zachęcić użytkownika usług płatniczych do zgłaszania swojemu dostawcy usług płatniczych bez zbędnej zwłoki każdej kradzieży lub utraty instrumentu płatniczego, a tym samym aby zmniejszyć ryzyko nieautoryzowanych transakcji płatniczych, użytkownik powinien ponosić odpowiedzialność wyłącznie do kwoty o bardzo ograniczonej wysokości, chyba że użytkownik ten działał w nieuczciwych zamiarach lub dopuścił się rażącego zaniedbania w tym zakresie. W tym kontekście kwota w wysokości 50 EUR wydaje się być odpowiednia do zapewnienia zharmonizowanego i wysokiego poziomu ochrony użytkowników w Unii. Płatnik nie powinien ponosić odpowiedzialności, jeżeli nie mógł zdawać sobie sprawy z utraty, kradzieży lub przywłaszczenia instrumentu płatniczego. Ponadto od momentu zgłoszenia dostawcy usług płatniczych przez użytkownika tego, że mogło dojść do nieuprawnionego użycia jego instrumentu płatniczego, użytkownik usług płatniczych nie powinien być zobowiązany do pokrycia żadnych dalszych strat wynikających z nieuprawnionego użycia tego instrumentu. Niniejsza dyrektywa powinna pozostawać bez uszczerbku dla odpowiedzialności dostawców usług płatniczych za bezpieczeństwo techniczne ich produktów*".

Jak jasno wynika z przytoczonego powyżej fragmentu, ustawodawca unijny dopuszcza zatem zwolnienie się z obowiązku niezwłocznego zwrotu przez dostawcę kwoty nieautoryzowanej transakcji płatniczej, w przypadku gdy istnieje prawdopodobieństwo działania płatnika **w nieuczciwych zamiarach**. Przy tak określonej intencji ustawodawcy unijnego nie można zdaniem Rzecznika inaczej odszyfrować znaczenia, użytego w art. 16 dyrektywy oraz art. 46 ust. 1 u.u.p., słowa „oszustwo" niż **oszustwo płatnika lub oszustwo z jego udziałem** (np. *friendly fraud*).

Treść motywu 71, w tym przede wszystkim wyróżnione zdanie, ma ogromne znaczenie w interpretacji przepisów dyrektywy PSD II, gdyż pokazuje intencje unijnego prawodawcy, którego naczelnym celem było zapewnienie unijnym konsumentom odpowiedniego poziomu ochrony w przypadku wystąpienia nieautoryzowanych transakcji płatniczych i coraz powszechniejszych oszustw. Unijny ustawodawca zdecydował się zatem na wprowadzenie ogólnej zasady zwrotu środków w przypadku występowania nieautoryzowanej transakcji płatniczych, co ma zwiększyć poziom ochrony klienta, a obowiązki związane z ewentualnym dowodzeniem faktu prawidłowej

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

autoryzacji transakcji, rażącego naruszenia obowiązków umownych czy nawet umyślnego doprowadzenia do nieautoryzowanej transakcji nałożył na dostawcę.

Zdaniem Rzecznika Finansowego jedyną podstawą do wstrzymania się dostawcy płatnika ze zwrotem środków nieautoryzowanej transakcji płatniczej po jej zgłoszeniu lub wykryciu na podstawie art. 46 ust. 1 u.u.p. jest podejrzenie oszustwa rozumianego jako oszustwo klienta lub oszustwo z jego udziałem. Dodatkowo podejrzenie to musi znaleźć odzwierciedlenie w poinformowaniu o tym fakcie właściwych organów oraz musi zostać udokumentowane.

> **W praktyce oznacza to, że jeśli bank nie poinformuje organów ścigania o próbie oszustwa ze strony klienta, to powinien zwrócić klientowi środki zgodnie z zasadą D+1.**

Można założyć, że gdyby instytucje finansowe respektowały wytyczne płynące z dyrektywy PSD II oraz jej wspomnianego motywu 71, do Rzecznika Finansowego powinny trafiać wyłącznie osoby, które potrzebują wsparcia merytorycznego na etapie przedsądowym lub sądowym, w sytuacji, w której to one są oskarżone (niesłusznie) o oszustwo. W praktyce Rzecznika Finansowego takie sprawy się nie pojawiają. Wnioski klientów dotyczą sytuacji, w której bank przedłuża okres oczekiwania na zwrot środków bądź też wprost odmawia takiego zwrotu mimo braku podstaw do zarzucenia klientowi oszustwa lub rażącego niedbalstwa.

Niedochowanie terminu zgłoszenia nieautoryzowanej transakcji

Dostawca ma prawo nie wypłacić niezwłocznie kwoty nieautoryzowanej transakcji płatniczej pomimo zgłoszenia przez użytkownika, jeżeli zgłoszenie to zostało dokonane z przekroczeniem ustawowego terminu. Użytkownik powinien powiadomić niezwłocznie dostawcę o stwierdzonych nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcjach płatniczych. Jeżeli z jakichś względów użytkownik nie dokonał zgłoszenia niezwłocznie, to zgodnie z art. 44 ust. 1 u.u.p. może to zrobić w terminie maksymalnie 13 miesięcy od dnia obciążenia rachunku płatniczego albo od dnia, w którym transakcja miała być wykonana. Po upływie tego terminu roszczenia użytkownika względem dostawcy z tytułu nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcji płatniczych **wygasają**. Co oznacza, że dostawca może się wówczas uchylić od zwrotu użytkownikowi kwoty nieautoryzowanej transakcji.

Z powyższej analizy wynika, że procedura działania osoby, która stwierdzi kradzież środków ze swojego konta powinna wyglądać tak jak na poniższym schemacie.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

KTOŚ UKRADŁ PIENIĄDZE?
Z TWOJEGO KONTA INTERNETOWEGO

Rzecznik Finansowy
www.rf.gov.pl

JAK NAJSZYBCIEJ POINFORMUJ

- SWÓJ BANK
- ZESPÓŁ CERT.PL (www.incydent.cert.pl),
- NAJBLIŻSZĄ JEDNOSTKĘ POLICJI **(KONIECZNIE WEŹ ZAŚWIADCZENIE!).**

*Niezależnie od informacji o kradzieży zgłoś się do swojego banku z **żądaniem zwrotu pieniędzy.***

ZASADA D+1

Zgodnie z tą zasadą, powinieneś otrzymać zwrot skradzionych pieniędzy nie później niż do końca dnia roboczego od stwierdzenia wystąpienia nieautoryzowanej transakcji lub zgłoszenia tego faktu.

Wstrzymanie zwrotu jest możliwe tylko w przypadku, gdy Twój bank ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać TWOJE oszustwo i poinformuje o tym na piśmie organy powołane do ścigania przestępstw.

JEŚLI BANK NIE ZWRÓCI CI ŚRODKÓW,
ZŁÓŻ REKLAMACJĘ!

15 dni roboczych
w takim czasie klient powinien otrzymać odpowiedź na reklamację usługi płatniczej.

Pamiętaj! Będziesz musiał zwrócić pieniądze bankowi, jeśli ***BANK UDOWODNI***, że:

- *Transakcja była **wykonana** przez Ciebie i próbowałeś oszukać bank.*
- ***Umyślnie** lub wskutek **rażącego niedbalstwa** naruszyłeś obowiązki użytkownika. Należą do nich:*

  ***niezwłoczne** zgłaszanie faktu kradzieży środków lub nieuprawnionego dostępu osób trzecich do konta,*

  korzystanie z konta zgodnie z zasadami określonymi w umowie,

  przechowywanie indywidualnych danych uwierzytelniających z zachowaniem należytej staranności i nieudostępnianie ich osobom nieuprawnionym.

UPRAWDOPODOBNIENIE ≠ UDOWODNIENIE

W razie sporu z bankiem na tym tle, możesz skorzystać ze wsparcia Rzecznika Finansowego. Jeśli dojdzie do sporu sądowego tzw. istotny pogląd w sprawie może przedstawić Urząd Ochrony Konkurencji i Konsumentów lub Rzecznik Finansowy.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa

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

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

d) Nowe terminy rozpatrywania reklamacji

Dyrektywa PSD II, a w ślad za nią polska ustawa o usługach płatniczych, wprowadziły nowe terminy rozpatrywania reklamacji usług płatniczych dla użytkowników będących osobami fizycznymi. Dostawcy mieli sześciomiesięczne *vacatio legis* na dostosowanie się do nowych regulacji w tym zakresie, stąd obowiązują one od dnia 20 grudnia 2018 r.

Zgodnie z nowymi przepisami do rozpatrywania reklamacji składanych przez użytkownika będącego osobą fizyczną stosuje się przepisy ustawy z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym[7], z pewnymi odmiennościami w szczególności w zakresie terminu rozpatrzenia reklamacji.

Przed wejściem w życie nowych przepisów dostawców będących podmiotami rynku finansowego w rozumieniu ustawy o Rzeczniku Finansowym obowiązywał standardowy termin rozpatrywania reklamacji przez podmioty rynku finansowego, określony w ustawie o Rzeczniku Finansowym – wynoszący 30 dni kalendarzowych.

Ustawa o usługach płatniczych wprowadziła zasadę, że dostawca udziela odpowiedzi na reklamację w terminie 15 dni roboczych od dnia jej otrzymania. Tylko w szczególnie skomplikowanych przypadkach, uniemożliwiających rozpatrzenie reklamacji termin ten może ulec wydłużeniu do 35 dni roboczych od dnia otrzymania reklamacji. Warto jednak podkreślić, że dostawca, który chciałby skorzystać z możliwości przedłużenia terminu odpowiedzi na reklamację, musi w ciągu wspomnianych powyżej 15 dni roboczych przekazać klientowi informację:

- wyjaśniającą przyczyny opóźnienia,
- wskazującą okoliczności, które muszą zostać ustalone w celu rozpatrzenia sprawy,
- określającą termin rozpatrzenia reklamacji i udzielenia odpowiedzi, nie dłuższy niż 35 dni roboczych od dnia otrzymania reklamacji.

Zasadniczo odpowiedź musi być udzielona w postaci papierowej. Istnieje możliwość przekazania jej na innym trwałym nośniku informacji (np. w dokumencie PDF, załączonym do wiadomości wysłanej drogą e-mailową), ale tylko po uzgodnieniu z użytkownikiem.

Celem zachowania terminów, o których mowa powyżej, wystarczy wysłanie odpowiedzi przed ich upływem, a w przypadku odpowiedzi udzielonych na piśmie – nadanie w placówce pocztowej operatora wyznaczonego w rozumieniu art. 3 pkt 13 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe[8].

[7] Dz. U. z 2018 r. poz. 2038 z późn. zm., dalej: u.r.f. lub ustawa o Rzeczniku Finansowym.
[8] Dz. U. z 2018 r. poz. 2188 z późn. zm.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

Warto podkreślić, że wprowadzone do ustawy o usługach płatniczych nowe przepisy (art. 15a–15d u.u.p.) dotyczące reklamacji usług płatniczych należy postrzegać jako *lex specialis* w stosunku do ustawy o Rzeczniku Finansowym, o ile podmiotem wnoszącym reklamację jest osoba fizyczna. W miejsce rozwiązań przewidzianych przepisami ustawy o Rzeczniku Finansowym stosuje się nowe regulacje wynikające z przepisów ustawy o usługach płatniczych. Pozostałe przepisy ustawy o Rzeczniku Finansowym, które nie zostały zastąpione nowymi przepisami ustawy o usługach płatniczych, będą nadal musiały być stosowane przez podmioty rynku finansowego. Dotyczy to w szczególności art. 3 u.r.f. – forma reklamacji i miejsce jej złożenia, art. 4 u.r.f. – informacja o procedurze składania reklamacji w umowie, art. 8 u.r.f. – sankcja w przypadku niedotrzymania terminu odpowiedzi na złożoną reklamację, art. 9 u.r.f. – treść odpowiedzi na reklamację, art. 10 u.r.f. – pouczenie w przypadku nieuwzględnienia roszczeń klienta.

Podobnie pamiętać należy, że jeżeli ustawa o usługach płatniczych wprowadziła jakieś regulacje, które nie są przewidziane w ustawie o Rzeczniku Finansowym, to powinny być one przez dostawców uwzględniane. Dotyczy to przykładowo art. 15a ust. 5 i 6 u.u.p., które dotyczą nałożonego na dostawców obowiązku stosowania procedur reklamacyjnych w odniesieniu do użytkowników z każdego z państw członkowskich, w których dostawca oferuje usługi, oraz dostępności procedur w językach urzędowych państw członkowskich, w których dostawca oferuje daną usługę płatniczą. Można powiedzieć zatem, że ustawy te w zakresie reklamacji użytkownika będącego osobą fizyczną wzajemnie się uzupełniają.

Poniżej schemat pokazujący jak liczyć termin odpowiedzi na reklamację usługi płatniczej.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

3. Postępowanie dostawców usług płatniczych w praktyce Rzecznika Finansowego

Analiza dotychczasowego sposobu postępowania dostawców w przypadku nieautoryzowanej transakcji płatniczej oraz rozpatrywania reklamacji płatników wskazuje, że podmioty rynku finansowego generalnie przyjmują zupełnie inną interpretację opisanych powyżej przepisów. Przy czym warto podkreślić, że konkluzja ta płynie z wniosków o tzw. postępowanie interwencyjne Rzecznika Finansowego. Istnieją jednak podmioty, które przyjmują punkt widzenia zbieżny ze stanowiskiem prezentowanym przez Rzecznika Finansowego.

W przypadku zgłoszenia przez płatnika nieautoryzowanej transakcji płatniczej zasadniczo dostawcy odmawiają zwrotu kwoty nieautoryzowanej transakcji płatniczej, powołując się na art. 46 ust. 3 lub art. 46 ust. 2 u.u.p. Stosowana przez podmioty argumentacja w większości zatem dotyczy doprowadzenia przez płatnika do nieautoryzowanej transakcji płatniczej w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 u.u.p., lub też wystąpienia transakcji płatniczej będącej skutkiem posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub przywłaszczenia instrumentu płatniczego.

Innymi słowy, głównym motywem powtarzającym się w argumentacji dostawców jest wina lub rażące niedbalstwo użytkownika przy posługiwaniu się instrumentem płatniczym, w szczególności polegające na udostępnianiu świadomie (lub nie) danych autoryzacyjnych instrumentu płatniczego, na przykład danych do logowania czy kodów autoryzacyjnych transakcji.

W ocenie podmiotów skutkuje to pełną odpowiedzialnością płatnika za nieautoryzowaną transakcję i eliminuje odpowiedzialność dostawcy usług płatniczych. W większości przypadków twierdzenia te nie są zasadniczo w żaden sposób udowodnione, gdyż podmioty poprzestają jedynie na ogólnikowym wskazaniu faktu zarejestrowania uwierzytelnienia i autoryzacji transakcji.

Na uwagę zwraca argumentacja niektórych banków, które poprzestają na odwołaniu się do założeń autoryzacji transakcji (powołując się na własne procedury i regulaminy bądź lakonicznie odwołując się do brzmienia ustawy) i wskazują – bez odniesienia do indywidualnych okoliczności sprawy – że dane takie jak login, dane identyfikacyjne czy numer telefonu do haseł SMS powinny być znane jedynie posiadaczowi rachunku. Z tak lakonicznej argumentacji, ograniczającej się jedynie do przywołania właściwych zasad postępowania, można *de facto* wysnuć wniosek, że każdy klient zgłaszający brak autoryzacji transakcji, który nie wskazuje okoliczności nadzwyczajnych czy też nie przedstawia dowodów na ocenę sytuacji przemawiającą na jego korzyść, nie

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

dochowuje należytej staranności (działanie kwalifikujące się jako rażące niedbalstwo), bowiem dostawca automatycznie przyjmuje, że doszło do niezachowania tajemnicy danych służących do logowania do platformy internetowej czy też niewłaściwego użycia narzędzi lub technologii do uzyskiwania kodów jednorazowych oraz informacji umożliwiających bezpieczne korzystanie z usług dostawcy.

Abstrahując od wskazanej wcześniej tezy Rzecznika, że ocena stopnia współodpowiedzialności płatnika za nieautoryzowaną transakcję powinna być dokonywana przez sąd w ramach procesu dowodowego, to wyjaśnienia podmiotów – formułowane również w ramach prowadzonych przez Rzecznika Finansowego postępowań – nie respektują w żaden sposób przerzuconego na te instytucje ciężaru dowodu wynikającego z art. 45 u.u.p. Jednym słowem, dostawcy nie przedstawiają dowodów na to, że transakcja płatnicza została autoryzowana i prawidłowo zapisana w systemie lub że płatnik umyślnie albo wskutek rażącego niedbalstwa doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie albo wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 u.u.p. W większości przypadków dostawcy uznają, że pewne zdarzenia, na przykład nieświadome logowanie na fałszywej stronie banku i udostępnienie w ten sposób danych do logowania, są rażącym naruszeniem obowiązku wynikającego z umowy, a dotyczącego nieudostępniania osobom trzecim danych niezbędnych do logowania. Bardzo często dostawcy wskazują, że transakcja została autoryzowana z uwagi na fakt potwierdzenia przez użytkownika transakcji unikatowym kodem, choć zgodnie z art. 45 ust. 3 u.u.p. fakt wykazania zarejestrowanego użycia instrumentu płatniczego nie jest wystarczający do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana, czyli płatnik wyraził na nią świadomą zgodę, albo że płatnik umyślnie lub wskutek rażącego niedbalstwa 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 u.u.p. Dostawca obowiązany jest udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej niż sam fakt autoryzacji kodem.

W przypadku przestępstw polegających na kopiowaniu instrumentu płatniczego (*skimming*) dostawcy w większości nie respektują ograniczenia odpowiedzialności płatnika za nieautoryzowane transakcje do wysokości 50 euro do momentu zgłoszenia faktu utraty lub kradzieży instrumentu płatniczego. Z analizy spraw wynika, że w tym przypadku dostawcy uznają winę płatnika, wskazując na nieodpowiednie przechowywanie lub zabezpieczenie instrumentu płatniczego albo udostępnienie kodu PIN. Jak wiadomo, obecnie przestępcy mają wiele metod na pozyskanie kodu PIN (np. zakładanie kamer lub nakładek na bankomatach). Niekiedy trudno jest użytkownikowi karty zorientować się, że gdy wstukuje on kod PIN, ktoś jednocześnie go podgląda i kod ten pozyskuje. Zasadniczo zatem dostawcy, w szczególności banki, w takich sytuacjach nie dokonują zwrotu kwot nieautoryzowanych transakcji płatniczych.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

> **Rzecznik Finansowy raz jeszcze podkreśla, że dostawcy (banki) nie przedstawiają jakichkolwiek dowodów na poparcie twierdzeń, jakoby płatnik przyczynił się swoim zachowaniem do wystąpienia nieautoryzowanej transakcji płatniczej.**

W tym miejscu należy zwrócić uwagę, iż ocena dowodów w polskim systemie prawnym została przypisana sądom powszechnym, stąd też dostawcy usług płatniczych będący zainteresowani pozytywnym dla nich rozstrzygnięciem sprawy w myśl zasady *Nemo iudex in causa sua* nie mogą być sędziami we własnej sprawie.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa

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

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

4. Z akt Rzecznika Finansowego

Ze skarg trafiających do Rzecznika Finansowego wynika, że mechanizmy oszustw związanych z transakcjami płatniczymi są bardzo różnorodne. Wydaje się, że w wielu sytuacjach trudno zarzucić klientom rażące niedbalstwo, a to właśnie jest zasadniczo głównym argumentem dostawców odmawiających realizacji obowiązku zwrotu kwoty nieautoryzowanej transakcji. Okazuje się, że nawet użyczenie telefonu osobie będącej w potrzebie może skończyć się zainfekowaniem złośliwym oprogramowaniem.

PRZYKŁAD:

Z informacji przekazanych przez wnioskodawcę wynikało, że na lotnisku w Polsce użyczył telefonu obcemu mężczyźnie, który wykonał jedno połączenie. Z opisu sprawy można wnosić, że najprawdopodobniej doszło wtedy do zainfekowania telefonu złośliwym oprogramowaniem. Klient posiadał aplikację bankową i na ten telefon były przesyłane wiadomości SMS z kodami potwierdzającymi transakcje. Niepokój klienta wzbudziły pojawiające się komunikaty, świadczące o logowaniu się do serwisu banku z żądaniem hasła. Zaniepokojony klient udał się do placówki banku. Tam pracownicy sprawdzili historię rachunku i nie stwierdzili żadnych obciążeń. Jak napisał klient: „Słowa, że czasami się tak dzieje, tylko uśpiły moją czujność." Okazało się jednak, że tego dnia oszuści wykonali pięć przelewów na łączną kwotę 39 019 zł. Zdaniem klienta tylko przełożenie karty SIM do drugiego telefonu (wykonane z własnej inicjatywy) pozwoliło mu uchronić resztę pieniędzy przed kradzieżą.

Z praktyki Rzecznika Finansowego wynika, że przed kradzieżą środków nie zawsze zabezpiecza też ustalanie różnego rodzaju limitów dotyczących liczby transakcji czy wartości przelewanych środków. Niestety, przestępcy przejmując kontrolę nad serwisem transakcyjnym ofiary, dokonują modyfikacji niezbędnych do wytransferowania wszystkich środków dostępnych na koncie.

PRZYKŁAD:

W jednej ze spraw wytransferowano kwotę 9 861,49 zł. Było to możliwe dzięki temu, że w serwisie bankowości elektronicznej najpierw zdefiniowano nowy numer rachunku jako tzw. zaufany. Następnie zmieniono limit na rzecz odbiorców zaufanych z 500 zł na 9930 zł. Obie czynności zostały potwierdzone kodem SMS, choć poszkodowany nie otrzymał ich na swój telefon.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

Rzecznik Finansowy odnotowuje też przypadki, w których ofiara oszustwa nie tylko straciła pieniądze posiadane na koncie, ale przestępcy zaciągnęli nawet w jej imieniu pożyczkę. Jest to możliwe w sytuacji, w której po przejęciu kontroli nad aplikacją mobilną lub uzyskaniu dostępu do panelu klienta ze strony internetowej można łatwo zaciągnąć tzw. kredyt „na klik". Niestety, Rzecznik Finansowy zaobserwował również przypadki, w których bank nie wstrzymuje się z żądaniem spłaty rat takiego kredytu przez klienta, choćby do czasu wyjaśnienia sprawy. Dopiero interwencje Rzecznika przynosiły zmianę decyzji w tym zakresie.

PRZYKŁAD:

Jak opisywała wnioskodawczyni, oszuści internetowi najprawdopodobniej przy użyciu specjalnego oprogramowania przejęli kontrolę nad jej telefonem. Oprogramowanie to wymusiło fikcyjną aktualizację systemu operacyjnego telefonu. Ponadto pozwalało sprawcom przechwytywać wiadomości SMS z kodami autoryzacyjnymi, umożliwiającymi zlecenie operacji bankowych. Na koniec aplikacja przywróciła ustawienia fabryczne telefonu, niszcząc w ten sposób ślady przestępstwa. Proces ten trwał około godziny. W tym czasie przestępcy zlecili przelew wszystkich środków, jakie były na koncie, a dodatkowo zaciągnęli kredyty na kwotę 13 600 zł, które to środki wytransferowali.

W niektórych sprawach przestępcy korzystają z faktu, że do konta są podpięte karty kredytowe czy debetowe i korzystają z możliwości zlecenia przelewów z tych rachunków.

PRZYKŁAD:

Jedna z klientek wskazywała, że kiedy doszło do włamania na jej konto, była w pracy i nie dokonywała żadnych transakcji. Nie otrzymywała na swój telefon żadnych SMS-ów z hasłami. Straciła 6070 zł funduszy zgromadzonych na koncie, kartę kredytową obciążono na łączną kwotę 17 700 zł, a kartę debetową na 2 000 zł.

W innej sprawie przestępcy przejęli kontrolę zarówno nad telefonem ofiary, jak i serwisem transakcyjnym na stronie internetowej. Tu należy zaznaczyć, że sprawa była przedmiotem tak interwencji Rzecznika Finansowego, jak i cieszyła się zainteresowaniem mediów. Ostatecznie bank zmienił swoje stanowisko i wyraził gotowość polubownego rozwiązania sporu. Uzasadnił to jednak „wieloletnią

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

współpracą z klientem". Warto podkreślić, że również w innych pozytywnie zakończonych interwencjach Rzecznika Finansowego pojawia się takie uzasadnienie. Niektóre banki po prostu informują o zmianie decyzji, jednocześnie przypominając (zresztą zgodnie z prawdą), że reklamacje rozpatrzone pozytywnie dla klienta nie wymagają uzasadnienia faktycznego i prawnego.

PRZYKŁAD:

Klient po zalogowaniu do serwisu transakcyjnego stwierdził, że ktoś w jego imieniu zawarł umowę pożyczki i wykonał dyspozycję przelewu. Pożyczka opiewała na kwotę 17 900 zł. Następnie w kolejnych logowaniach zostały zmienione limity wypłat dziennych i miesięcznych. Ostatecznie wytransferowano z konta kwotę 15 930 zł.

Mimo dość różnych stanów faktycznych sprawy te mają jeden element wspólny: do końca nie wiadomo, kto dokonał autoryzacji transakcji. Przypomnijmy, że zgodnie z art. 45 u.u.p. dostawca usług ma udowodnić, że to klient autoryzował daną transakcję. Przy czym – zdaniem Rzecznika Finansowego – dostawca musi przywołać inne dowody niż sam fakt prawidłowego skorzystania z procedur autoryzacji przewidzianych umową. Nie oznacza to bowiem jeszcze, że transakcję autoryzował płatnik.

Same banki w korespondencji przyznają, że „prawdopodobnie" doszło na przykład do przekazania przez klienta danych potrzebnych do wykonania i autoryzowania transakcji. Warto jednak podkreślić, że nie przedstawiają na to żadnych dowodów. A przypomnijmy, że przepis ustawy mówi jasno o „udowodnieniu", a nie o „uprawdopodobnieniu".

Banki w swoich stanowiskach wskazują też na „ewentualny udział osób trzecich oraz przestępczy charakter zdarzenia", *de facto* potwierdzając, że to nie klient dokonał autoryzacji transakcji. W ocenie Rzecznika Finansowego w takiej sytuacji bank powinien zwrócić klientowi utraconą kwotę i ewentualnie domagać się jej zwrotu, jeśli postępowanie wykaże, że płatnik umyślnie albo wskutek rażącego niedbalstwa 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 u.u.p.

Na zakończenie warto odnotować przypadki, które co prawda nie były przedmiotem skarg kierowanych do Rzecznika Finansowego, jednak doskonale pokazują, że do zainfekowania telefonu czy komputera lub przejęcia nad nimi kontroli może dochodzić nawet bez żadnych działań ze strony klienta. Rzecznik Finansowy ma nadzieję, że

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

brak informacji o odrzuceniu reklamacji klienta w tego typu przypadkach oznacza, że zostały one rozpatrzone zgodnie w wolą klienta.

Jednym z takich przypadków był atak z maja 2019 r. na użytkowników aplikacji WhatsApp. Warto odnotować ten przypadek, jako pokazujący, jak łatwo stać się ofiarą hakerów bez winy ze strony posiadacza telefonu. Jak donoszą media: „Hakerzy w swoich działaniach wykorzystali funkcję połączeń głosowych. Osoby zaatakowane mogły zobaczyć dwa nieodebrane połączenia z nieznanego numeru. Połączenie nie musiało zostać odebrane, żeby zainfekować telefon. U niektórych osób znikało ono też z historii połączeń, dlatego użytkownicy mogą nie wiedzieć, że ich telefon został zainfekowany oprogramowaniem, które przejmowało kontrolę nad systemem operacyjnym telefonu. Programiści WhatsAppa zwracają uwagę, że użytkownicy w przypadku ataku nie mogli nic zrobić, poza odinstalowaniem aplikacji”[9].

Innym przykładem jest sygnalizowany m.in. przez Prezesa Urzędu Komunikacji Elektronicznej[10] problem z nadużyciami wskutek podmiany kart SIM. Był on opisywany w ten sposób: „Przestępcy, którzy znają dane użytkownika, w tym jego numer telefonu oraz dane banku, w którym posiada on rachunek, w sposób nieuprawniony dokonują przekierowania połączeń na swoje numery. Inną metodą jest podszywanie się pod użytkownika w salonie operatora i wyłudzanie duplikatu karty SIM. W ten sposób dochodzi do przejęcia numeru telefonu, który kolejno wykorzystywany jest do sparowania mobilnych aplikacji bankowych instalowanych na telefonach i realizacji przelewów bankowych lub przejęcia kont poczty elektronicznej użytkowników czy kont w serwisach społecznościowych. Przestępcy mają dzięki temu dostęp do autoryzacji lub uwierzytelnienia operacji bankowych, np. w formie kodów otrzymywanych SMS-em”.

[9] https://www.rmf24.pl/fakty/swiat/news-atak-hakerski-na-uzytkownikow-whatsappa-moze-za-nim-stac-izr,nId,2989866.
[10] https://www.uke.gov.pl/akt/prezes-uke-ostrzega-przed-naduzyciami-z-podmiana-kart-sim,114.html.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

5. Podsumowanie

Rzecznik Finansowy dostrzega fundamentalny problem związany z procedurą stosowaną przez dostawców usług płatniczych w przypadku zgłoszenia przez użytkownika faktu wystąpienia nieautoryzowanej transakcji płatniczej. Jak wskazuje niniejsza Analiza, celem zmiany przepisów w tym zakresie dokonanej przez ustawodawcę unijnego, a w ślad za nim również polskiego, jest nie tylko zwiększenie ochrony konsumenta (użytkownika usług płatniczych), ale również zmniejszenie ryzyka wystąpienia nieautoryzowanych transakcji na rynku płatniczym. Ten cel w ocenie ustawodawcy unijnego najlepiej będzie realizowany poprzez przerzucenie w dużej mierze odpowiedzialności za wystąpienie nieautoryzowanej transakcji płatniczej na dostawców usług płatniczych. To oni dysponują zarówno wiedzą, jak i zapleczem technicznym pozwalającym na wprowadzanie procedur minimalizujących ryzyko wystąpienia nieautoryzowanej transakcji płatniczej. Takie podejście wymusza także na dostawcach usług płatniczych stosowanie wysokich standardów bezpieczeństwa oraz mechanizmów zabezpieczających przed ryzykiem występowania nieautoryzowanych transakcji płatniczych.

Z wniosków trafiających do Rzecznika Finansowego wynika, że banki jako zasadniczy dostawcy usług płatniczych ignorują wytyczne wynikające z unijnych dyrektyw i polskiego prawa.

> **Chodzi w szczególności o brak niezwłocznego zwrotu utraconych przez klienta środków w terminie D+1. Ponadto odmowa zwrotu następuje najczęściej jedynie w oparciu o uprawdopodobnienie (a nie udowodnienie!) czy też wyłącznie na podstawie twierdzeń banku o winie, umyślności lub rażącym niedbalstwie klienta jako okolicznościach uzasadniających tę odmowę.**

Bank samodzielnie dokonuje oceny odpowiedzialności płatnika związanej z wystąpieniem nieautoryzowanej transakcji płatniczej, działając przy tym – jako zainteresowany zwolnieniem się z odpowiedzialności – w roli sędziego we własnej sprawie. Warto w tym miejscu zwrócić uwagę na fakt, że to dostawca ma więcej możliwości i środków, w szczególności technicznych i technologicznych, które umożliwiają mu prześledzenie historii nieautoryzowanej transakcji. Takich możliwości klient nie posiada.

Z analizy spraw zgłoszonych do Rzecznika Finansowego wynika, że procedura stosowana przez banki przewiduje zwrot środków dopiero po wielotygodniowym czy nawet wielomiesięcznym postępowaniu wyjaśniającym, przeprowadzonym przez organy ścigania. Innymi słowy, banki uzależniają zwrot środków będących przedmiotem nieautoryzowanej transakcji płatniczej od zakończeniu postępowania karnego w sprawie oszustwa. Jakie ma to konsekwencje dla poszkodowanego klienta?

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa
biuro@rf.gov.pl
www.rf.gov.pl
facebook.com/Rzecznik Finansowy
Tel. 22 333 73 **26**
22 333 73 **27**
fax. 22 333 73 **29**

Jak pokazaliśmy na wybranych przykładach, w skrajnym przypadku klient nie tylko traci wszystkie posiadane pieniądze, ale też zaciągany jest w jego imieniu dług. Co ma zrobić w takiej sytuacji? Za co kupić jedzenie, jak opłacić rachunki?

> **Wydaje się, że intencją prawodawców było wdrożenie rozwiązania, które zapewnia szybki zwrot utraconych środków (zgodnie z zasadą D+1), co pozwala nie pozostawiać klientów bez środków do życia. W związku z tym opóźnienie w zwrocie środków powinno być wyjątkiem, a nie regułą, jak ma to miejsce w dzisiejszej praktyce banków.**

Zresztą co warto podkreślić, większość występujących na rynku nieautoryzowanych transakcji płatniczych wiąże się z oszustwem. Przyjęcie retoryki banków, że w przypadku każdego oszustwa, o którym bank zawiadomi organy ścigania, dostawca jest zwolniony z obowiązku niezwłocznego zwrotu środków, czyni nową regulację martwą i pozbawioną celu.

> **Dlatego też w ocenie Rzecznika Finansowego wstrzymanie się ze zwrotem kwoty nieautoryzowanej transakcji musi wynikać z uzasadnionych i należycie udokumentowanych postaw pozwalających podejrzewać oszustwo ze strony klienta.**

Zasada niezwłocznego zwrotu środków po zgłoszeniu przez użytkownika lub wykryciu przez dostawcę nieautoryzowanej transakcji płatniczej wynika – w ocenie Rzecznika Finansowego – zarówno z wykładni literalnej, jak i celowościowej przepisów dyrektywy PSD II oraz przepisów krajowych, w szczególności art. 46 ust. 1 u.u.p. Z kolei by na klienta nałożyć częściową lub pełną odpowiedzialność za utratę środków, dostawca (bank) powinien udowodnić (a nie uprawdopodobnić) przykładowo fakt celowego lub świadomego udostępnienia przez klienta haseł czy loginów do konta osobom trzecim. Nieprzypadkowo to na dostawców nałożono większe obowiązki związane z bezpieczeństwem transakcji. Jest to zgodne z podejściem zakładającym, że za jakość wytworzonego narzędzia odpowiada jego wytwórca. Jeśli systemy czy procedury stosowane przez dostawców umożliwiają wystąpienie nieautoryzowanych transakcji lub dostawcy nie stosują zabezpieczeń na odpowiednim poziomie, przykładowo związanych z monitoringiem występowania nieautoryzowanych transakcji płatniczych, to powinni oni ponosić większą odpowiedzialność za nieautoryzowane transakcje.

Warto podkreślić, że dostawca ma prawo wyrażenia żądania zwrotu przekazanych klientowi kwot, jeśli spełni wyżej wspomniane warunki dowodowe. Przypomnijmy, że opóźnienie w zwrocie środków klientowi jest możliwe tylko w sytuacji, w której o podejrzeniu oszustwa ze strony klienta dostawca poinformuje na piśmie w sposób udokumentowany organy ścigania. W takim przypadku klientowi będzie groziła też odpowiedzialność karna. Wydaje się więc, że ryzyko sankcji cywilnej (zwrot środków plus koszty ewentualnego postępowania sądowego) i karnej (wyrok za oszustwo) niweluje ryzyko tzw. hazardu moralnego ze strony klientów.

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa

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

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

Istotnym problemem – o czym już była mowa – jest też brak dodatkowych procedur zabezpieczających przed dokonywaniem nieautoryzowanych transakcji w ramach serwisu transakcyjnego. Analizowane przez Rzecznika Finansowego przypadki pokazują, że przestępcy przejmujący kontrolę nad kontem ofiary zwykle mają możliwość dokonywania wszelkich zmian. Ustawione przez klienta limity, dotyczące na przykład liczby czy wartości przelewów dziennych, są łatwo zmieniane przez oszustów, jeśli tylko są one zbyt niskie, żeby opróżnić co do grosza konto klienta. W praktyce dają więc one złudne poczucie bezpieczeństwa.

> **Systemy bankowości internetowej i mobilnej powinny zatem być wyposażone w mechanizmy zabezpieczające przed takimi sytuacjami.**

Być może wiązałoby się to z większymi ograniczeniami dla klienta, na przykład w formie dodatkowej autoryzacji lub kolejnego uwierzytelnienia, jednakże w ocenie Rzecznika Finansowego wobec coraz częstszych ataków oszukańczych wprowadzenie takich ograniczeń jest wskazane.

Problemem jest też możliwość zaciągnięcia kredytu „na klik" czy obciążenia karty kredytowej lub debetowej (co zostało opisane w poprzednim rozdziale). Wydaje się, że tu także wskazane byłoby wprowadzenie dodatkowych procedur zabezpieczających. Zdaniem Rzecznika Finansowego być może należałoby rozważyć rozwiązania poprawiające bezpieczeństwo kosztem szybkości przeprowadzania transakcji. Byłoby to zgodne z zasadą *security first*, o której stosowanie przy wdrażaniu nowoczesnych rozwiązań Rzecznik Finansowy nieustannie apeluje.

Tradycyjnie analizy Rzecznika Finansowego są przekazywane wszystkim podmiotom zainteresowanym poruszaną problematyką. Rzecznik liczy w szczególności na dobrą współpracę z Komisją Nadzoru Finansowego, która z mocy prawa otrzymuje od Rzecznika Finansowego również informację o liczbie i charakterze skarg wskazujących na naruszenia ustawy o usługach płatniczych według stanu na koniec każdego półrocza. Rzecznik ma nadzieję, że bieżąca wymiana informacji na temat dostrzeganych problemów pozwoli na koordynację działań poprawiających poziom bezpieczeństwa osób korzystających z usług płatniczych.

Niniejsza Analiza jest pierwszą próbą oceny problemów związanych z nieautoryzowanymi transakcjami płatniczymi. Rzecznik Finansowy liczy, że doprowadzi ona do zmiany praktyki i zachowań dostawców usług płatniczych. Jednocześnie Rzecznik rozważa podjęcie badania ankietowego wśród dostawców, którego wynik może wesprzeć inicjatywy mające na celu zmiany systemowe.

Opracowanie: Izabela Dąbrowska-Antoniak

Współpraca: Paulina Krakowska, Marcin Jaworski

Rzecznik Finansowy
Al. Jerozolimskie 87
02 – 001 Warszawa

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

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