OBOWIĄZKI ZWIĄZANE Z KORZYSTANIEM Z INSTRUMENTU PŁATNICZEGO ORAZ ROZKŁAD ODPOWIEDZIALNOŚCI MIĘDZY DOSTAWCĄ A UŻYTKOWNIKIEM W PRZYPADKU TRANSAKCJI NIEAUTORYZOWANYCH

SYGN. WIB PAB 19/2022

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

PROGRAM ANALITYCZNO BADAWCZY

Warszawa, 30 listopada 2022 r.

PROGRAM ANALITYCZNO BADAWCZY

O Raporcie

Raport **Obowiązki związane z korzystaniem z instrumentu płatniczego oraz rozkład odpowiedzialności między dostawcą a użytkownikiem w przypadku transakcji nieautoryzowanych** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy:

Raport przygotowany przez zespół w składzie:

prof. dr hab. Marek Kolasiński

dr Marcin Olechowski

dr Wojciech Iwański

dr Mateusz Blocher

PROGRAM ANALITYCZNO BADAWCZY

O Programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie i cyberbezpieczeństwo**
- **Zdolność banków do finansowania gospodarki**
- **Bankowość spółdzielcza**
- **Rynek nieruchomości**
- **Zielony ład i finansowanie energetyki odnawialnej**
- **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt:

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl

Spis treści

I. Wprowadzenie

1. Z dniem 12 stycznia 2016 r. weszła w życie druga dyrektywa w sprawie usług płatniczych (**PSD2**)[1]. PSD2 została implementowana do polskiego porządku prawnego poprzez nowelizację ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (**UUP**). Należy na wstępie zaznaczyć, że PSD2 jest dyrektywą harmonizacji pełnej (maksymalnej)[2]. Nowelizacja weszła w życie co do zasady w dniu 20 czerwca 2018 r. W praktyce jednak wiele przepisów zostało objętych dodatkowymi okresami przejściowymi. W efekcie, nowe rozwiązania prawne, wynikające z implementacji PSD2 w Polsce, w pełni funkcjonują w obrocie począwszy od 14 września 2019 r. Od tej daty stosuje się bowiem wymogi w zakresie silnego uwierzytelniania użytkownika (**SCA**), co stanowiło jeden z zasadniczych obszarów nowej regulacji.

2. Zmiany wprowadzone do UUP w związku z implementacją PSD2 dotyczyły m.in. zasad rozkładu odpowiedzialności między dostawcą usług płatniczych i użytkownikiem w przypadku wystąpienia **nieautoryzowanych transakcji płatniczych**. Zasady tej odpowiedzialności zostały kompleksowo uregulowane w art. 46 UUP, który zaostrzył obowiązki dostawców usług płatniczych w zakresie zwrotów kwot transakcji nieautoryzowanych:

   (i) art. 46 ust. 1 UUP dookreślił termin na dokonanie przez dostawcę zwrotu kwoty transakcji nieautoryzowanej jako nie dłuższy niż jeden dzień roboczy (tzw. termin D+1) oraz doprecyzował przesłanki uzasadniające brak dokonania takiego zwrotu, pomimo że transakcja ma charakter nieautoryzowany[3];

   (ii) nowy art. 46 ust. 1a i 1c UUP określiły zasady dokonywania zwrotu kwoty transakcji nieautoryzowanej w przypadku transakcji, które są inicjowane za pośrednictwem dostawcy świadczącego usługę inicjowania transakcji płatniczej (PIS) oraz uregulowały zasady wzajemnych rozliczeń między takim dostawcą, a dostawcą prowadzącym rachunek płatniczy;

   (iii) art. 46 ust. 2 UUP obniżył granicę odpowiedzialności płatnika za nieautoryzowane transakcje płatnicze do kwoty 50 EUR (z kwoty 150 EUR) oraz zawęził przesłanki aktualizujące ograniczony zakres odpowiedzialności płatnika (przy czym chodzi tutaj o zasadę ogólną);

   (iv) nowy art. 46 ust. 2a UUP określił dodatkowe przesłanki skutkujące wyłączeniem współodpowiedzialności płatnika z tytułu wystąpienia nieautoryzowanych transakcji płatniczych; oraz

   (v) nowy art. 46 ust. 4a UUP wprowadził pełną odpowiedzialność dostawcy usług płatniczych w przypadku, gdy nie wymaga on SCA (z zastrzeżeniem umyślnego działania płatnika).

3. Jednocześnie na przestrzeni ostatnich kilku lat doszło do znacznego rozwoju usług bankowości elektronicznej i zdecydowanego wzrostu liczby uczestników korzystających z tego typu rozwiązań. Według danych z 2019 r. aż 96% wszystkich polskich internautów używa narzędzi bankowości elektronicznej[4]. Wybuch pandemii COVID-19 (SARS-CoV-2) jest uważany za jeden z czynników dodatkowo wzmacniających popularność bankowości internetowej w latach 2020-2022. Według danych Mastercard[5], pod koniec 2020 r. ponad połowa Polaków deklarowała częstsze wykonywanie transakcji w Internecie oraz mobilnie niż przed pandemią. Z kolei według raportu Związku Banków Polskich[6] za 4 kwartał 2021 r. obecnie już około 21 mln Polaków aktywnie korzysta

[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.

[2] Por. art. 107 ust. 1 PSD2.

[3] Nie zmienia to jednak faktu, że dostawca nie musi dokonywać zwrotu w terminie D+1, jeżeli zachodzi domniemanie autoryzacji transakcji zgodnie z art. 45 ust. 1 UUP. Taki przypadek – tj. gdy należy przyjmować autoryzowany charakter transakcji – nie mieści się bowiem w hipotezie normy wynikającej z art. 46 ust. 1 UUP. Przepis ten dotyczy wyłącznie przypadków wystąpienia transakcji nieautoryzowanej. Zob. publikację pt. „Analiza dotycząca implementacji dyrektywy PSD2 do polskiego porządku prawnego w zakresie udowodnienia autoryzacji transakcji przez dostawcę usług płatniczych" z dnia 22 stycznia 2021 r., sygn. WIB PAB 13/2021. Odmienny pogląd prezentuje jednak Prezes Urzędu Ochrony Konkurencji i Konsumentów – por. m.in. Stanowisko Prezesa UOKiK w sprawie interpretacji przepisów ustawy z 19 sierpnia 2011 r. o usługach płatniczych w zakresie dotyczącym nieautoryzowanych transakcji płatniczych z dnia 16 listopada 2022 r., opubl. na stronie UOKiK (https://uokik.gov.pl/download.php?plik=26783 ; dostęp 17 listopada 2022 r.).

[4] *A. Marciniak*, Polacy cenią sobie bankowość mobilną i online za wygodę i szybkość, oczekują bezpieczeństwa, Mastercard, 5 czerwca 2019 r., https://www.mastercard.com/news/europe/pl-pl/centrum-prasowe/informacje-prasowe/pl-pl/2019/czerwiec/badanie-mastercard-polacy-cenia-sobie-bankowosc-mobilna-i-online-za-wygode-i-szybkosc-oczekuja-bezpieczenstwa/, data dostępu: 1.09.2022 r.

[5] Mastercard, "The global state of pay", https://www.mastercard.com/news/insights/2020/the-global-state-of-pay/, data dostępu: 1 września 2022 r.

[6] Związek Banków Polskich, „NetB@nk, bankowość internetowa i mobilna, płatności bezgotówkowe", 31 września 2022 r., https://www.zbp.pl/Aktualnosci/Wydarzenia/Raport-NetB@nk-Q4-2021-Czwarty-kwartal-2021-z-dalszym-wzrostem-potencjalu-bankowosci-elektronicznej, data dostępu: 1 września 2022 r.

z usług bankowości internetowej, co oznacza wzrost tej grupy użytkowników o 1,6 % w stosunku do roku poprzedniego. W tym samym raporcie odnotowano także 17% wzrost liczby użytkowników bankowych aplikacji mobilnych w stosunku do roku ubiegłego.

4. Nadal jednak świadomość użytkowników usług bankowości elektronicznej co do niebezpieczeństw i zagrożeń dla tych usług, w szczególności w zakresie teleinformatycznym i socjotechnicznym, wydaje się niewystarczająca. Nowe metody i schematy oszustw pojawiają się w błyskawicznym tempie. Jednocześnie nawyki i przyzwyczajenia klientów korzystających z rozwiązań bankowości elektronicznej nie rozwijają się wystarczająco szybko, aby odpowiednio zapobiegać tego typu oszustwom. Z tego względu na przestrzeni ostatnich lat dostawcy usług płatniczych, w tym w szczególności dostawcy bankowi, położyli szczególny nacisk na kampanie informacyjne i edukacyjne, których celem jest zwiększenie świadomości klientów co do potencjalnych zagrożeń i oczekiwanego od klientów poziomu ostrożności[7].

5. Tymczasem pomimo zdecydowanego wzmocnienia zabezpieczeń w zakresie zdalnego korzystania z rozwiązań bankowości elektronicznej – co m.in. miało związek z koniecznością dostosowania się dostawców usług płatniczych do wymogów SCA – oraz pomimo prowadzonych w tym zakresie kampanii edukacyjnych, coraz częściej można usłyszeć o przypadkach dotkliwych oszustw, wskutek których klienci banków utracili nierzadko cały swój majątek[8]. Wachlarz zdarzeń, do których dochodzi w praktyce obrotu, jest w zasadzie nieograniczony. Niekiedy są to przypadki, gdy do nieautoryzowanej transakcji płatniczej dochodzi wskutek uchybień w procedurach bezpieczeństwa dostawcy usług płatniczych. **Często zdarza się jednak, że przyczyną wystąpienia takich transakcji są daleko idące zaniedbania klientów w zakresie zasad bezpiecznego korzystania z instrumentów płatniczych.** Niekiedy zaś problem leży pomiędzy zaniedbaniami po stronie dostawcy i zaniedbaniami po stronie użytkownika.

6. Główną osią niezgody między sektorem bankowym i organami konsumenckimi, w tym Rzecznikiem Finansowym oraz Prezesem Urzędu Ochrony Konkurencji i Konsumentów, są praktyki banków w zakresie trybu dokonywania zwrotów kwot transakcji nieautoryzowanych (art. 46 ust. 1 UUP)[9]. Zagadnienie to nie jest jednak przedmiotem niniejszej publikacji. Problematykę tę poruszaliśmy w odrębnym opracowaniu z ubiegłego roku przygotowanym dla Fundacji Warszawski Instytut Bankowości[10]. Niniejsze opracowanie jest jednak z tą tematyką nierozłącznie związane, dotyka ono bowiem zasad rozkładu odpowiedzialności między użytkownikiem i dostawcą w przypadku wystąpienia transakcji nieautoryzowanej oraz ewentualnych podstaw takiej odpowiedzialności, w zależności od stopnia uchybień po stronie użytkownika w związku z korzystaniem z instrumentu płatniczego. Z uwagi na przedmiot obu opracowań, wnioski w nich zawarte należy czytać więc łącznie.

[7] Przykładami takich kampanii informacyjnych mogą być kolejne edycje kampanii mBank S.A. pt. „Ludzie są niesamowici" (https://pl.media.mbank.pl/171550-mbank-kolejny-raz-o-bezpieczenstwie-w-sieci-to-niesamowite-jak-przebiegli-sa-internetowi-przestepcy, data dostępu 1 września 2022 r.) lub działania informacyjne PKO BP S.A. (https://bankomania.pkobp.pl/finanse/bezpieczenstwo/jak-oszusci-kradna-pieniadze-z-kont-czyli-vishing-phishing-i-smishing-w-akcji/, data dostępu 1 września 2022 r.)

[8] MM/GP, 15 lipca 2022 r.: „Chciała kupić akcje, straciła oszczędności życia", TVN24, https://tvn24.pl/pomorze/bydgoszcz-chciala-kupic-akcje-stracila-oszczednosci-zycia-5788475, data dostępu 2 września 2022 r., KEP (2022, 23 czerwca); „Straciła 60 tys. złotych oszczędności. Oszukał ją fałszywy pracownik banku", TVP3 Kielce, https://kielce.tvp.pl/60902960/stracila-60-tys-zlotych-oszczednosci-oszukal-ja-falszywy-pracownik-banku, data dostępu 2 września 2022 r.; por. także przykłady podobnych sytuacji przywoływane przez Rzecznika Finansowego, https://rf.gov.pl/2021/09/23/rzecznik-finansowy-interweniuje-w-sprawie-nieautoryzowanych-transakcji/, data dostępu 2 września 2022 r.

[9] Przykładem aktywności wskazanych organów mogą być prowadzone przez Prezesa UOKiK postępowania wyjaśniające w sprawie transakcji nieautoryzowanych. W dniu 18 lipca 2022 r. urząd poinformował o postawieniu zarzutów naruszenia zbiorowych interesów konsumentów 5 bankom oraz o kontynuowaniu postępowań wyjaśniających wobec 13 innych banków. Zob. UOKiK, Transakcje nieautoryzowane – zarzuty wobec 5 banków, https://uokik.gov.pl/aktualnosci.php?news_id=18708, data dostępu: 31 sierpnia 2022 r.

[10] Publikacja pt. „Analiza dotycząca implementacji dyrektywy PSD2 do polskiego porządku prawnego w zakresie udowodnienia autoryzacji translacji przez dostawcę usług płatniczych" z dnia 22 stycznia 2021 r., sygn. WIB PAB 13/2021.

II. Instrumenty płatnicze – obowiązki dostawcy i użytkownika

7. Usługi płatnicze wiążą się przede wszystkim z obowiązkami nałożonymi na dostawców świadczących takie usługi (np. banki). To na dostawcy spoczywa ciężar zapewnienia, że usługi te będą wykonywane zgodnie z wymogami regulacyjnymi, w tym, że dostawca zapewni odpowiednie mechanizmy bezpieczeństwa związane z dostępem do rachunków płatniczych, wykonywaniem transakcji i przeprowadzaniem innych czynności, które mogą rodzić ryzyko oszustwa lub podobnych nadużyć. Jednak ustawodawca wprowadził także pewne obowiązki spoczywające na klientach (użytkownikach usług płatniczych), które mają kluczowe znaczenie dla bezpieczeństwa usług płatniczych. Prawidłowa realizacja tych obowiązków może z kolei bezpośrednio przekładać się na rozkład odpowiedzialności między dostawcą i użytkownikiem w przypadku wystąpienia nieautoryzowanej transakcji płatniczej.

8. Obowiązki użytkowników usług płatniczych można najogólniej podzielić na obowiązki o charakterze **ostrożnościowym** oraz obowiązki o charakterze **lojalnościowo-informacyjnym.**

9. W przypadku obowiązków o charakterze ostrożnościowym, pożądane zachowanie użytkownika usług płatniczych wyznacza art. 42 UUP. Zgodnie z art. 42 ust. 1 pkt 1 UUP, użytkownik uprawniony do korzystania z określonego instrumentu płatniczego (np. karty płatniczej albo instrumentu bankowości internetowej lub mobilnej)[11], **ma obowiązek korzystać z tego instrumentu zgodnie z umową ramową**, a więc – w pewnym uproszczeniu – zgodnie z zawartą między użytkownikiem i dostawcą umową o usługi płatnicze, która reguluje zasady wykonywania transakcji płatniczych oraz (często) zasady prowadzenia rachunku płatniczego (bankowego)[12]. Z kolei zgodnie z art. 42 ust. 2 UUP, w celu spełnienia tego obowiązku, użytkownik, z chwilą otrzymania instrumentu płatniczego, **powinien podjąć niezbędne środki służące zapobieżeniu naruszenia indywidualnych danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym**.

10. Natomiast obowiązki o charakterze lojalnościowo-informacyjnym w praktyce sprowadzają się do obowiązku szybkiego reagowania przez użytkownika na zidentyfikowane nieprawidłowości i zagrożenia, tak, aby umożliwić dostawcy usług płatniczych podjęcie kroków ograniczających negatywne następstwa takich zdarzeń. W tym celu, zgodnie z art. 42 ust. 1 pkt 2 UUP, użytkownik ma obowiązek **zgłaszać niezwłocznie dostawcy** (lub innemu podmiotowi wskazanemu przez dostawcę) **stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu**. Ponadto, zgodnie z art. 44 ust. 1 UUP, użytkownik powinien niezwłocznie powiadomić dostawcę o stwierdzonych nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcjach płatniczych. Jeżeli nie dokona tego w terminie 13 miesięcy od dnia obciążenia rachunku płatniczego (w przypadku transakcji nieautoryzowanych[13]), to przysługujące mu roszczenia względem dostawcy wygasają[14].

11. Prawidłowe wykonywanie przez użytkowników obciążających ich obowiązków stanowi jeden z filarów bezpieczeństwa usług płatniczych. Dotyczy to w szczególności obrotu zdalnego, gdzie dostawca nie ma realnych narzędzi, aby sprawować bieżącą „kontrolę" i pieczę nad sposobem korzystania z instrumentów płatniczych przez użytkownika. Kontrola ta sprawowana jest niejako pośrednio, poprzez wprowadzenie odpowiednich mechanizmów zabezpieczających i związanych z nimi reguł – w szczególności procedur uwierzytelniania – służących weryfikacji ważności i poprawności używania konkretnego instrumentu płatniczego.

12. W doktrynie prawniczej wskazuje się, że celem wprowadzenia tych obowiązków jest ochrona bezpieczeństwa transakcji płatniczych i ograniczenie ryzyka, że dojdzie do wykonania transakcji nieautoryzowanych wskutek nieprawidłowego obchodzenia się przez użytkowników z instrumentami płatniczymi, naruszenia poufności indywidualnych danych uwierzytelniających albo zaniechania podjęcia środków zaradczych[15]. Zgodnie z motywem (69) do PSD2,

[11] Co do pojęcia „instrument płatniczy" por. szeroko *W. Iwański*, Instrument płatniczy, Monitor Prawa Bankowego 2022 r., nr 7–8.

[12] Definicję legalną pojęcia „umowa ramowa" zawiera art. 2 pkt 31 UUP. Pojęcia tego nie należy przy tym mylić z „umową ramową" w klasycznym rozumieniu prywatnoprawnym tj. umową organizującą proces zawierania umów wykonawczych w przyszłości. Umowa ramowa w rozumieniu UUP to samodzielne pojęcie normatywne.

[13] W przypadku, gdy użytkownik nie korzysta z rachunku płatniczego, termin ten liczy się od dnia wykonania nieautoryzowanych lub nienależycie wykonanych transakcji płatniczych albo od dnia, w którym transakcja płatnicza miała być wykonana.

[14] Tego typu obowiązki nie są nowością w prawie polskim. Por. przede wszystkim art. 728 § 3 KC, zgodnie z którym posiadacz rachunku bankowego jest obowiązany zgłosić bankowi niezgodność zmian stanu rachunku lub salda w ciągu czternastu dni od dnia otrzymania wyciągu z rachunku.

[15] Tak *T. Czech*, w: *K. Osajda* (red. serii), *J. Dybiński* (red. tomu), Ustawa o usługach płatniczych. Komentarz, Legalis 2022 r., wyd. 1, kom. do art. 42, nb 2.

obowiązek bezpiecznego przechowywania indywidualnych danych uwierzytelniających ma ogromne znaczenie dla ochrony środków pieniężnych użytkownika usług płatniczych i dla ograniczenia ryzyk związanych z oszustwami i nieuprawnionym dostępem do rachunku płatniczego. **Celem prawodawcy było więc to, aby ciężar czuwania nad bezpieczeństwem usług płatniczych był dzielony między dostawcami usług płatniczych i użytkownikami tych usług** – oczywiście przy zachowaniu odpowiedniej roli każdej z tych stron w obrocie gospodarczym. O ile dostawca ma obowiązek zapewnić właściwe rozwiązania technologiczne i mechanizmy służące zabezpieczeniu instrumentów płatniczych, w tym wykonywanych przy ich użyciu transakcji (takim mechanizmem jest chociażby konieczność stosowania SCA), **o tyle użytkownik ma obowiązek prawidłowego korzystania z tych zabezpieczeń i unikania sytuacji, w których zabezpieczenia te mogą zostać osłabione lub przełamane na skutek jego własnego zachowania**.

13. Konsekwencją tak skonstruowanego podziału zadań jest odpowiedni rozkład odpowiedzialności między dostawcą i użytkownikiem w przypadku nieautoryzowanych transakcji płatniczych. Domyślną regułą jest podział tej odpowiedzialności pomiędzy dostawcą i użytkownikiem, z tym, że odpowiedzialność użytkownika ogranicza się do kwoty 50 euro (art. 46 ust. 2 UUP). Reguła ta podlega jednak daleko idącym modyfikacjom – i to w obie strony. W określonych bowiem przypadkach to dostawca ponosi pełną odpowiedzialność za nieautoryzowaną transakcję płatniczą. Są jednak także takie sytuacje, gdy cały ciężar finansowy transakcji nieautoryzowanej spoczywa na użytkowniku. **Do zbioru przypadków, gdzie dochodzi do całkowitej odpowiedzialności użytkownika, należą właśnie sytuacje, gdy** płatnik doprowadził do **transakcji umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków związanych z korzystaniem z instrumentu** płatniczego (art. **46 ust. 3 w zw. z art. 42 UUP)**.

III. Obowiązki ostrożnościowe użytkownika

14. Jak wskazaliśmy powyżej, odpowiednie korzystanie przez użytkownika z instrumentu płatniczego stanowi jeden z kluczowych elementów bezpieczeństwa wykonywanych transakcji płatniczych. **W tym zakresie ustawodawca oczekuje od użytkownika, że będzie przestrzegał określonych reguł bezpieczeństwa (art. 42 UUP)**. Przy czym uregulowanie zasad korzystania z instrumentu płatniczego pozostawiono samym stronom – dostawcy i użytkownikowi – wskazując, że użytkownik powinien używać instrumentu **zgodnie z umową ramową**. Taki zabieg należy uznać za celowy. Odmienne rozwiązanie wymagałoby nadmiernie kazuistycznych uregulowań normatywnych. Nieprzypadkowo znaczna część przepisów prawa usług płatniczych formułowana jest z uwzględnieniem zasady neutralności technologicznej[16]. Na przykładzie korzystania z instrumentu płatniczego jasne jest bowiem, że zasady bezpieczeństwa i przyjęte w tym zakresie środki prewencyjne zależeć będą od szeregu zindywidualizowanych okoliczności, w tym charakteru konkretnego instrumentu płatniczego, zakresu jego funkcjonalności, podatności na oszustwa i zagrożenia określonego typu etc., czego nie może prawidłowo uchwycić regulacja odgórna. **Dlatego też kluczową rolę w tym zakresie odgrywają relacje „poziome" (prywatnoprawne), a więc zasady, na które umawiają się dostawca usług płatniczych (często wydawca instrumentu płatniczego) oraz użytkownik (płatnik)**.

15. Należy przy tym zwrócić uwagę, że „zasady korzystania z instrumentu płatniczego" to **kategoria dynamiczna, zmienna w czasie i poddana ciągłej ewolucji**. Usługi płatnicze jako takie, a w szczególności instrumenty płatnicze, podlegają od ponad dwóch dekad nieustannemu, bardzo prężnemu rozwojowi. Niemal codziennie w ofercie dostawców pojawiają się nowe rozwiązania płatnicze, które pozwalają klientom jeszcze pełniej i łatwiej korzystać z dobrodziejstw nowoczesnego rynku płatności. Wprowadzenie takich rozwiązań przeważnie stanowi odzew na potrzeby samego rynku, w tym na oczekiwania formułowane przez użytkowników usług płatniczych. Odgórne

[16] Por. np. motyw (4) rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji. Zasada ta opiera się na założeniu, że aby zapewnić neutralność pod względem technologicznym stosowanych rozwiązań płatniczych, nie należy w przepisach prawa wymagać stosowania konkretnej technologii i konkretnych rozwiązań technicznych.

uregulowanie obowiązków związanych z korzystaniem z instrumentów płatniczych w akcie prawnym (rangi dyrektywy, ustawy czy rozporządzenia) wymagałoby więc częstych, regularnych przeglądów pod kątem aktualności przewidzianych tam regulacji. Taki zabieg – choć formalnie możliwy – w praktyce byłby trudny do realizacji i zapewne mniej skuteczny niż pozostawienie tego obszaru regułom umownym.

16. **Z powyższych względów, istotną rolę w kształtowaniu pożądanej praktyki rynkowej, w tym pożądanego zachowania użytkowników, odgrywają zasady korzystania z instrumentów płatniczych, stanowiące element umów ramowych**. W praktyce są to wzorce umowne szczegółowo regulujące zasady świadczenia usług płatniczych przez określonych dostawców. Podkreślić należy, że system prawny dobrze zabezpiecza użytkowników przed hipotetycznym, nadmiernym rozszerzaniem obowiązków użytkowników. Wprawdzie treść stosunku kontraktowego na badanej płaszczyźnie ustala dostawca, a użytkownik często nie zapoznaje się z nim na etapie kontraktowania, stosowną ochronę zapewniają mu jednak prywatnoprawne klauzule generalne i instytucje prawa ochrony konsumenta oraz działania organów administracyjnych (Prezesa Urzędu Ochrony Konkurencji i Konsumentów, Rzecznika Finansowego). Na zasadach ogólnych – postanowienia umowy ramowej podlegają bowiem ocenie pod kątem abuzywności. Ponadto, granice ustaleń w zakresie zasad korzystania z instrumentów płatniczych wyznacza przepis art. 42 ust. 3 UUP, który stanowi, że umowa ramowa powinna zawierać **obiektywne, niedyskryminujące i proporcjonalne** postanowienia dotyczące wydawania i użytkowania instrumentu płatniczego.

17. W tym miejscu zaakcentować należy **ogromne znaczenie właściwego sformułowania przedmiotowych regulaminów.** Praktyka ochrony zbiorowych interesów konsumentów w Polsce jest wysoce interwencjonistyczna. Nie należą do rzadkości przypadki, gdy tylko nieznacznie niewłaściwe, w warstwie semantycznej, ujęcie określonego obowiązku w regulaminie, skutkuje jego wyeliminowaniem z treści stosunku prawnego łączącego użytkownika i dostawcę. Potrzebę zachowania przez dostawcę daleko idącej ostrożności na tej płaszczyźnie uznać należy za tym większą, że kontrola abstrakcyjna wzorców umownych jest w praktyce często oderwana od realiów obrotu i nie istnieje osiągalna szansa na przewidzenie jej wyniku. Wskazać należy też, że standardy ustalone w obrocie konsumenckim są nierzadko przenoszone poza jego granice. Polska judykatura jest przy tym przychylna odwoływaniu się do klauzul generalnych, a względom aksjologicznym przypisuje się bardzo duże znaczenie w procesie wykładni postanowień wzorców umownych.

18. Zasady korzystania z instrumentu płatniczego są kategorią **zmienną w czasie**. Naturalnej ewolucji ulegają instrumenty płatnicze i społeczno-gospodarcze otoczenie, w którym są one wykorzystywane. W tym kontekście wskazać należy, iż pewnej ewolucji podlega także m.in. **model należycie starannego użytkownika**, który ma zasadnicze znaczenie dla ustalenia tego, czy w konkretnej sytuacji poszkodowany dołożył należytej staranności i czy jego zachowanie zaklasyfikować można jako rażące niedbalstwo. Zmianom temporalnym nie podlega stopień pilności, jakiej można oczekiwać od użytkownika, lecz model zachowań, jakich rozsądnie wymagać można od użytkownika w zmienionych okolicznościach.

19. Rekonstrukcja modelu należycie starannego użytkownika w konkretnych okolicznościach może być zadaniem bardzo trudnym, a próby dokonywania uogólnień obarczone są znacznym ryzykiem błędów. Bez niebezpieczeństwa ich popełnienia stwierdzić można, że bezpodstawne jest oczekiwanie od użytkownika, iż będzie on poświęcał szczególną uwagę analizie kryminalistycznej oszustw występujących przy dokonywaniu transakcji płatniczych. Z drugiej jednak strony, uprawnionym jest wymaganie, aby użytkownik prezentował **rozsądny poziom zainteresowania zagrożeniami**, które wiążą się z wykonywaniem transakcji. W praktyce, na badanej płaszczyźnie, często przydatne może być wykorzystywanie rozwiązań wypracowanych w sprawach konsumenckich w zakresie rekonstrukcji modelu przeciętnego konsumenta, choć oczywiście pamiętać należy, iż nie każdemu użytkownikowi przysługuje ochrona, jaką system prawny zapewnia konsumentom.

20. Uzasadnione jest przy tym wiązanie przez dostawców usług płatniczych zakresu i charakteru oczekiwanych od użytkowników wymagań ostrożnościowych z **rodzajem instrumentu płatniczego**.

21. Poniżej, w ujęciu tabelarycznym, prezentujemy zestawienie często występujących obecnie obowiązków ostrożnościowych, których zachowania wymaga się od użytkowników w obrocie konsumenckim:

Nr	Obowiązki ostrożnościowe użytkownika
1.	Logowanie oraz wykonywanie dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście, z użyciem indywidualnych instrumentów uwierzytelniających.
2.	Zachowanie w tajemnicy informacji zapewniających bezpieczne korzystanie z usług bankowości elektronicznej, w tym informacji przekazanych bankowi dla celów weryfikacji oraz nieudostępnianie i nieujawnianie innym osobom (w tym osobom bliskim lub pracownikom banku) instrumentów uwierzytelniających.
3.	Nieprzekazywanie danych uwierzytelniających osobom trzecim, zwłaszcza podczas przychodzącej rozmowy telefonicznej, nawet jeżeli rozmówca przedstawia się jako pracownik banku.
4.	Nieprzekazywanie danych uwierzytelniających na stronach internetowych lub w aplikacjach, do których dostęp uzyskiwany jest przez linki przesłane przez nieznane osoby, w tym także na stronach internetowych zawierających znaki graficzne banku.
5.	Nieprzekazywanie danych uwierzytelniających w celu otrzymania płatności przy transakcjach na odległość.
6.	Należyte zabezpieczenie urządzeń i oprogramowania, których klient używa w celu korzystania z usług bankowości elektronicznej, tj. stosowanie legalnego i zaktualizowanego oprogramowania, stosowanie aktualnego oprogramowania antywirusowego, antyspamowego oraz typu *firewall*, najnowszych wersji przeglądarek internetowych oraz niestosowanie aplikacji automatyzujących.
7.	Przechowywanie karty płatniczej oraz kodu PIN z zachowaniem należytej staranności i zasad bezpieczeństwa, np. nieprzechowywanie ich razem, niezapisywanie kodu PIN w telefonie, komputerze lub notatniku.
8.	Przechowywanie indywidualnych danych uwierzytelniających bankowości elektronicznej z zachowaniem należytej staranności, w tym obowiązek nieprzechowywania ich razem.
9.	Nieudostępnianie karty płatniczej lub kodu PIN osobom nieuprawnionym, w tym bliskim lub pracownikom banku.
10.	Nieudostępnianie danych karty w celach innych niż dokonanie transakcji, zgłoszenie reklamacji czy zgłoszenie zablokowania karty.
11.	Pobieranie aplikacji mobilnej banku wyłącznie z autoryzowanego sklepu z aplikacjami.
12.	Nieotwieranie oraz nieodpowiadanie na wiadomości e-mail od nieznanych nadawców oraz nieotwieranie nieznanych plików z załączników.
13.	Zachowywania fabrycznych zabezpieczeń urządzeń mobilnych.

* opracowanie własne[17]

[17] Zestawienie przygotowane na podstawie obowiązujących w czasie przygotowania niniejszej analizy dostępnych publicznie regulaminów świadczenia usług bankowych lub regulaminów kart płatniczych wybranych polskich banków zidentyfikowanych przez Komisję Nadzoru Finansowego jako banki o znaczeniu systemowym. Zestawienie zostało przygotowane na podstawie następujących regulaminów: (i) Szczegółowe Warunki Świadczenia Usług Bankowości Elektronicznej i Usługi Bankowości Telefonicznej oraz Składania Oświadczeń w PKO Banku Polskim SA (wersja obowiązująca od 4.08.2018 r.); (ii) Regulamin Kart Płatniczych dla Klientów Indywidualnych w PKO Banku Polskim SA (wersja obowiązująca od 1.03.2022 r.); (iii) Regulamin Rachunków Bankowych Banku Pekao S.A. dla Osób Fizycznych (wersja obowiązująca od 1.09.2021 r.); (iv) Regulamin debetowych kart płatniczych dla klientów indywidualnych Santander Bank Polska SA (wersja obowiązująca od 1.07.2022 r.); (v) Regulamin kart debetowych dla osób fizycznych i klientów Private Banking w ramach bankowości detalicznej mBanku S.A. (wersja obowiązująca od 30.08.2022 r.); (vi) Regulamin świadczenia przez ING Bank Śląski S.A. usług w ramach prowadzenia rachunków płatniczych dla osób fizycznych (wersja obowiązująca od 29.08.2022 r.); (vii) Ogólne Warunki Umowy Rachunków Bankowych, Karty oraz Elektronicznych Kanałów Dostępu BNP Paribas SA (wersja obowiązująca od 22.11.2022 r.); (viii) Regulamin Rachunków Bankowych Banku Handlowego SA (wersja obowiązująca od 15.09.2022 r.); (ix) Regulamin rachunków bankowych, kart debetowych oraz usługi bankowości elektronicznej i usługi bankowości telefonicznej w Getin Noble Bank SA dla osób fizycznych nieprowadzących działalności gospodarczej (wersja obowiązująca od 1.01.2022 r.); (x) Regulamin Ogólny Świadczenia Usług Bankowych dla Osób Fizycznych w Banku Millennium S.A. (wersja obowiązująca od 25.04.2022 r.); (xi) Regulamin Kart Kredytowych w Banku Polskiej Spółdzielczości SA (wersja obowiązująca od 19.04.2021 r.).

22. Niezależnie od uregulowania obowiązków ostrożnościowych użytkownika, dostawcy często umieszczają w umowach ramowych dodatkowe klauzule informacyjne, które mają na celu ostrzec użytkownika przed potencjalnymi niebezpieczeństwami w zakresie korzystania z usług płatniczych, takie jak:

Nr	Dodatkowe klauzule informacyjne
1.	Informacja, że bank nigdy nie wymaga ujawnienia przez użytkownika haseł do bankowości elektronicznej (poza miejscami do tego przeznaczonymi w ramach bankowości internetowej).
2.	Informacja, że bank nigdy nie wymaga zainstalowania dodatkowego oprogramowania oprócz aplikacji banku pobranej z autoryzowanego sklepu z aplikacjami mobilnymi.
3.	Ostrzeżenie, że w przypadku instalacji aplikacji pozwalającej na zdalny dostęp do urządzenia, narażone zostają dane użytkownika i środki na jego rachunku.
4.	Zalecenie ochrony haseł używanych do logowania w aplikacjach i na stronach internetowych, jeżeli zostały w nich zapisane dane karty.
5.	Zalecenie zachowania ostrożności w przypadku płatności kartą w Internecie, wprowadzania PIN-u w terminalu lub bankomacie.
6.	Zalecenie monitorowania poprawności stanu rachunku.

* *opracowanie własne*[18]

IV. Obowiązki lojalnościowo-informacyjne użytkownika

23. Nie mniej doniosłe znaczenie mają nałożone na użytkownika usług płatniczych obowiązki o charakterze lojalnościowo-informacyjnym. Obowiązki te wprawdzie nie zapobiegają bezpośrednio (inaczej niż obowiązki ostrożnościowe) ryzyku wystąpienia oszustwa i naruszenia bezpieczeństwa usług płatniczych (choć w zależności od przypadku nie jest to wykluczone), ale mogą przyczynić się do częściowego ograniczenia tych zjawisk, w tym zmniejszenia wynikających z nich szkód (w majątku dostawcy usług płatniczych albo klienta).

24. Kluczowy w tym zakresie jest obowiązek, o którym mowa w art. 42 ust. 1 pkt 2 UUP. **Użytkownik powinien zgłaszać niezwłocznie dostawcy (lub podmiotowi wskazanemu przez dostawcę) stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu.**

25. Obowiązku tego nie należy mylić z obowiązkiem zgłaszania przez użytkownika roszczeń z tytułu niewykonanych, nienależycie wykonanych lub nieautoryzowanych transakcji płatniczych (art. 44 ust. 1 UUP). Pierwszy z tych obowiązków ukierunkowany jest na bezpieczeństwo usług

[18] Zestawienie przygotowane na podstawie obowiązujących w czasie przygotowania niniejszej analizy dostępnych publicznie regulaminów świadczenia usług bankowych lub regulaminów kart płatniczych wybranych polskich banków zidentyfikowanych przez Komisję Nadzoru Finansowego jako banki o znaczeniu systemowym. Zestawienie zostało przygotowane na podstawie następujących regulaminów: (i) Szczegółowe Warunki Świadczenia Usług Bankowości Elektronicznej i Usługi Bankowości Telefonicznej oraz Składania Oświadczeń w PKO Banku Polskim SA (wersja obowiązująca od 4.08.2018 r.); (ii) Regulamin Kart Płatniczych dla Klientów Indywidualnych w PKO Banku Polskim SA (wersja obowiązująca od 1.03.2022 r.); (iii) Regulamin Rachunków Bankowych Banku Pekao S.A. dla Osób Fizycznych (wersja obowiązująca od 1.09.2021 r.); (iv) Regulamin debetowych kart płatniczych dla klientów indywidualnych Santander Bank Polska SA (wersja obowiązująca od 1.07.2022 r.); (v) Regulamin kart debetowych dla osób fizycznych i klientów Private Banking w ramach bankowości detalicznej mBanku S.A. (wersja obowiązująca od 30.08.2022 r.); (vi) Regulamin świadczenia przez ING Bank Śląski S.A. usług w ramach prowadzenia rachunków płatniczych dla osób fizycznych (wersja obowiązująca od 29.08.2022 r.); (vii) Ogólne Warunki Umowy Rachunków Bankowych, Karty oraz Elektronicznych Kanałów Dostępu BNP Paribas SA (wersja obowiązująca od 22.11.2022 r.); (viii) Regulamin Rachunków Bankowych Banku Handlowego SA (wersja obowiązująca od 15.09.2022 r.); (ix) Regulamin rachunków bankowych, kart debetowych oraz usługi bankowości elektronicznej i usługi bankowości telefonicznej w Getin Noble Bank SA dla osób fizycznych nieprowadzących działalności gospodarczej (wersja obowiązująca od 1.01.2022 r.); (x) Regulamin Ogólny Świadczenia Usług Bankowych dla Osób Fizycznych w Banku Millennium S.A. (wersja obowiązująca od 25.04.2022 r.); (xi) Regulamin Kart Kredytowych w Banku Polskiej Spółdzielczości SA (wersja obowiązująca od 19.04.2021 r.).

płatniczych. Funkcja drugiego obowiązku jest inna – służy on zabezpieczeniu interesów finansowych klienta w związku z ewentualnymi nieprawidłowościami w świadczeniu usług płatniczych przez dostawcę.

26. Obowiązku tego nie należy także łączyć z przepisami o reklamacjach. Użytkownik ma **obowiązek zawiadomić dostawcę o zdarzeniu, które naraża na szwank bezpieczeństwo instrumentu płatniczego**. Możliwość złożenia reklamacji to z kolei przysługujące użytkownikowi uprawnienie wystąpienia do dostawcy z zastrzeżeniami dotyczącymi sposobu wykonania przez niego usług płatniczych (art. 2 pkt 24b UUP).

27. W celu umożliwienia użytkownikowi dokonywania zgłoszeń, o których mowa w art. 42 ust. 1 pkt 2 UUP, dostawcy usług płatniczych mają obowiązek zapewnić stałą dostępność odpowiednich środków komunikacji (art. 43 ust. 1 pkt 3 UUP). W praktyce dostawcy często zapewniają kanały kontaktu, które dostępne są 24 godziny na dobę, 7 dni w tygodniu[19]. Jednocześnie kanały te muszą być bezpłatne (art. 43 ust. 1 pkt 4a UUP), tak aby nie zniechęcać użytkowników do dokonywania zgłoszeń związanych z bezpieczeństwem usług płatniczych. Zakres obowiązków organizacyjnych nałożonych w tym względzie na dostawców świadczy o doniosłości, jaką ustawodawca przypisuje zgłoszeniom użytkowników. Niewątpliwie jest to jeden z filarów bezpieczeństwa całego rynku usług płatniczych.

28. Warto zwrócić uwagę, że zastrzeżony przez prawodawcę termin na dokonanie stosownego zgłoszenia przez użytkownika, **tj. niezwłocznie**, nie bez powodu został określony w ten właśnie sposób. Mowa bowiem o bezpieczeństwie usług płatniczych. Konieczność zawiadomienia dostawcy w sposób niezwłoczny oznacza, że użytkownik powinien skontaktować się z dostawcą **bez opóźnienia** będącego następstwem okoliczności, za które on odpowiada. W doktrynie prawniczej podkreśla się, że w tym konkretnie kontekście „niezwłocznie" **na ogół oznacza czas kilku godzin** – oczywiście o ile użytkownik dysponuje odpowiednimi środkami komunikacji z dostawcą i może łatwo ustalić sposób dokonania zgłoszenia[20]. Istotny dla realizacji tego obowiązku informacyjnego jest przy tym moment, w którym użytkownik zorientował się, że doszło np. do utraty przez niego instrumentu płatniczego, a nie moment, w którym faktycznie taka utrata nastąpiła.

29. **Prawidłowa realizacja omawianego tu obowiązku informacyjnego ma doniosłe znaczenie dla oceny zachowania klienta, w tym przypisania mu ewentualnej winy (umyślności, niedbalstwa lub rażącego niedbalstwa), w przypadku wystąpienia transakcji nieautoryzowanej.** Przykładowo: użytkownik, który zauważył, że utracił kartę płatniczą, powinien niezwłocznie zawiadomić o tym fakcie dostawcę (np. w ciągu kilku godzin od takiego spostrzeżenia). Jeżeli w wyniku takiego zdarzenia doszłoby następnie do wykonania transakcji nieautoryzowanej przy użyciu tej karty (przez osobę nieuprawnioną), a użytkownik nie dokonałby takiego zgłoszenia, dostawca mógłby mieć podstawy do stwierdzenia niedbalstwa, a czasami wręcz rażącego niedbalstwa po stronie użytkownika. Gdyby bowiem użytkownik zgłosił zdarzenie wcześniej, dostawca mógłby – przynajmniej w części przypadków – zapobiec wykonaniu takich transakcji. W praktyce obrotu zdarza się zaś, że użytkownicy ignorują ciążące na nich obowiązki informacyjne i dokonują stosownych zgłoszeń z opieszałością.

30. Poniżej, w ujęciu tabelarycznym, prezentujemy zestawienie najczęściej występujących obecnie obowiązków informacyjnych, których oczekuje się od użytkowników w obrocie konsumenckim:

[19] Np. mLinia oferowana przez mBank S.A. całą dobę, przez siedem dni w tygodniu, https://www.mbank.pl/kontakt/mlinia, data dostępu 1 września 2022 r.

[20] Tak *T. Czech*, w: *K. Osajda* (red. serii), *J. Dybiński* (red. tomu), Ustawa o usługach płatniczych. Komentarz, Legalis 2022 r., wyd. 1, kom. do art. 42, nb 20.1.

Nr	Obowiązki lojalnościowo-informacyjne użytkownika
1.	Niezwłoczne zgłoszenie bankowi utraty, kradzieży, przywłaszczenia, nieuprawnionego użycia lub dostępu do karty w serwisie telefonicznym, w oddziałach banku lub za pośrednictwem serwisu internetowego.
2.	Niezwłoczne zgłoszenie bankowi utraty, kradzieży, przywłaszczenia, nieuprawnionego użycia lub dostępu do instrumentów uwierzytelniających (kod PIN, kod CVC2/CVV2) w serwisie telefonicznym, w oddziałach banku lub za pośrednictwem serwisu internetowego.
3.	Niezwłoczne zgłoszenie bankowi stwierdzenia utraty, kradzieży, przywłaszczenia telefonu, na którym zainstalowana jest aplikacja mobilna i dodana karta zbliżeniowa w postaci wirtualnej lub aplikacja obca, w której zapisane są karty wydane przez bank.
4.	Zgłoszenie bankowi sytuacji poznania przez osobę trzecią danych karty płatniczej lub kodu PIN.

** opracowanie własne*[21]

V. Stopień zawinienia użytkownika

31. Prawidłowe wykonanie przez użytkownika omówionych wyżej obowiązków ostrożnościowych i lojalnościowo-informacyjnych ma doniosłe znaczenie prawne. Zależy bowiem od niego ciężar finansowy, jaki będzie ponosić użytkownik w przypadku wystąpienia transakcji nieautoryzowanej.

32. Zgodnie z art. 46 ust. 3 UUP, 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 UUP. Przepis ten wprowadza wyjątek od ogólnej reguły rozkładu odpowiedzialności, zgodnie z którą płatnik odpowiada za nieautoryzowane transakcje płatnicze jedynie do wysokości 50 euro jeżeli nieautoryzowana transakcja jest skutkiem posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub przywłaszczenia instrumentu płatniczego (art. 46 ust. 2 UUP). Do przypisania użytkownikowi odpowiedzialności konieczne jest jednak w każdym przypadku istnienie związku przyczynowego pomiędzy wystąpieniem transakcji nieautoryzowanej, a będącym skutkiem rażącego niedbalstwa naruszeniem obowiązków z art. 42 UUP, co wynika wprost z treści art. 46 ust. 3 UUP[22]. Przykładowo, jeżeli płatnikowi można co prawda zarzucić nieprawidłowości w przestrzeganiu obowiązków ostrożnościowych związanych z korzystaniem z karty płatniczej, ale okoliczności transakcji nieautoryzowanej dotyczą w konkretnym przypadku systemu bankowości internetowej i poleceń przelewu (a nie karty), to trudno jest przyjąć istnienie związku przyczynowego pomiędzy wystąpieniem transakcji nieautoryzowanej a naruszeniami po stronie płatnika.

[21] Zestawienie przygotowane na podstawie obowiązujących w czasie przygotowania niniejszej analizy dostępnych publicznie regulaminów świadczenia usług bankowych lub regulaminów kart płatniczych wybranych polskich banków zidentyfikowanych przez Komisję Nadzoru Finansowego jako banki o znaczeniu systemowym. Zestawienie zostało przygotowane na podstawie następujących regulaminów: (i) Szczegółowe Warunki Świadczenia Usług Bankowości Elektronicznej i Usługi Bankowości Telefonicznej oraz Składania Oświadczeń w PKO Banku Polskim SA (wersja obowiązująca od 4.08.2018 r.); (ii) Regulamin Kart Płatniczych dla Klientów Indywidualnych w PKO Banku Polskim SA (wersja obowiązująca od 1.03.2022 r.); (iii) Regulamin Rachunków Bankowych Banku Pekao S.A. dla Osób Fizycznych (wersja obowiązująca od 1.09.2021 r.); (iv) Regulamin debetowych kart płatniczych dla klientów indywidualnych Santander Bank Polska SA (wersja obowiązująca od 1.07.2022 r.); (v) Regulamin kart debetowych dla osób fizycznych i klientów Private Banking w ramach bankowości detalicznej mBanku S.A. (wersja obowiązująca od 30.08.2022 r.); (vi) Regulamin świadczenia przez ING Bank Śląski S.A. usług w ramach prowadzenia rachunków płatniczych dla osób fizycznych (wersja obowiązująca od 29.08.2022 r.); (vii) Ogólne Warunki Umowy Rachunków Bankowych, Karty oraz Elektronicznych Kanałów Dostępu BNP Paribas SA (wersja obowiązująca od 22.11.2022 r.); (viii) Regulamin Rachunków Bankowych Banku Handlowego SA (wersja obowiązująca od 15.09.2022 r.); (ix) Regulamin rachunków bankowych, kart debetowych oraz usługi bankowości elektronicznej i usługi bankowości telefonicznej w Getin Noble Bank SA dla osób fizycznych nieprowadzących działalności gospodarczej (wersja obowiązująca od 1.01.2022 r.); (x) Regulamin Ogólny Świadczenia Usług Bankowych dla Osób Fizycznych w Banku Millennium S.A. (wersja obowiązująca od 25.04.2022 r.); (xi) Regulamin Kart Kredytowych w Banku Polskiej Spółdzielczości SA (wersja obowiązująca od 19.04.2021 r.).

[22] Zgodnie z art. 46 ust. 3 UUP: *„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"*.

33. Co więcej, nie każde naruszenie dowolnego obowiązku nałożonego na użytkownika będzie wiązać się ze zwiększeniem jego odpowiedzialności. **Zależy to od postaci naruszenia oraz stopnia zawinienia użytkownika**.

34. Stopniowanie niedbalstwa użytkownika odbywa się przy wykorzystaniu kryterium ogólnej staranności wymaganej w stosunkach danego rodzaju (art. 355 §1 KC). Tutaj są to stosunki kreowane na gruncie umowy o świadczenie usług płatniczych (umowy ramowej). **Nie chodzi przy tym o staranność najwyższą, a o staranność ogólnie wymaganą.** Jest to pewne minimum, którego może oczekiwać wierzyciel (bank, dostawca) i które zapewnia dłużnikowi (użytkownikowi) brak odpowiedzialności, gdyby zobowiązania nie udało się wykonać[23]. **Zachowanie, które na niekorzyść odbiega od oczekiwanego wzorca, stanowi niedbalstwo**. **Jeżeli zaś różnica między zaistniałym zachowaniem a pożądanym jego wzorcem jest rażąca, należy mówić o rażącym niedbalstwie**[24]. W orzecznictwie sądów polskich przyjmuje się, że jeżeli określona osoba zachowała się w określonym miejscu i czasie w sposób odbiegający od właściwego dla niej miernika staranności, to o rażącym niedbalstwie będzie mowa wtedy, gdy niedochowane zostają minimalne (elementarne) zasady prawidłowego zachowania się w danej sytuacji, które to zasady są oczywiste dla większości rozsądnie myślących ludzi[25].

35. Zgodnie z przywołanym powyżej art. 46 ust. 3 UUP, do zwiększenia pułapu odpowiedzialności finansowej użytkownika w przypadku nieautoryzowanej transakcji płatniczej dochodzi wyłącznie w przypadku umyślnego doprowadzenia do takich transakcji albo umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków ostrożnościowych lub lojalnościowo-informacyjnych (art. 42 UUP). **„Zwykłe" niedbalstwo użytkownika w wykonaniu tych obowiązków nie pociąga za sobą zwiększenia jego odpowiedzialności**.

36. Nie jest kontrowersyjne twierdzenie, że z perspektywy praktyki obrotu kluczowe znaczenie ma tu przesłanka rażącego niedbalstwa. Wynika to stąd, że w dobie zelektronizowanego obrotu płatniczego, gdzie dominują relacje w pełni zdalne, wykazanie przez dostawcę, że płatnik umyślnie doprowadził do transakcji nieautoryzowanych albo umyślnie naruszył ciążące na nim obowiązki jest zazwyczaj bardzo trudne. W takich przypadkach, wykazanie przez dostawcę umyślnego doprowadzenia do transakcji nieautoryzowanej albo umyślnego naruszenia obowiązków wydaje się możliwe wyłącznie w tych przypadkach, gdzie klient wprost przyzna się do winy. Trudno bowiem sobie wyobrazić postępowanie dowodowe, gdzie dostawca w oparciu o dostępne dla niego materiały i informacje (np. treść reklamacji, dane systemowe co do zaksięgowanej transakcji, fakt prawidłowego uwierzytelnienia etc.) ustali faktyczny stosunek świadomości użytkownika do jego zamiaru (bezpośredniego lub ewentualnego). Wykazanie zamiaru ewentualnego (*dolus eventualis*) będzie być może nieco łatwiejsze niż zamiaru bezpośredniego (*dolus directus*), ale podobnie trudne w wymiarze dowodowym[26]. W praktyce mogą występować także przypadki, gdzie płatnik dopuszcza się jawnego oszustwa względem dostawcy usług płatniczych. Przypadki te należą jednak do rzadkości.

37. **Przedmiotem rzeczywistych sporów często jest natomiast zasadność przypisania użytkownikowi rażącego niedbalstwa.** Możliwe jest bowiem wykazanie, jakie konkretnie obowiązki zostały naruszone przez użytkownika w określonym przypadku. **Analizując całokształt okoliczności danej sprawy, możliwe jest także dokonanie oceny, jak uchybienia klienta odbiegają w konkretnym przypadku od pożądanego wzorca zachowania** (co stanowi o stopniu zawinienia użytkownika).

38. Należy przy tym wspomnieć, że **ocena** wagi naruszenia przez użytkownika obowiązków, o których mowa w art. 42 UUP, **może być dokonana przez dostawcę usług płatniczych**. **Będzie to zwykła ocena wykonania zobowiązania przez jedną ze stron tego zobowiązania.** Jeżeli dostawca uważa więc, że w określonych okolicznościach zwrot kwoty transakcji nie jest należny użytkownikowi, to dostawca ten może podjąć decyzję o odmowie takiego zwrotu[27]. Z tych powodów nieuzasadniona jest praktyka organów konsumenckich, które stoją na stanowisku, że

[23] Zob. *M. Gutowski*, w: *M. Gutowski* (red.), Kodeks cywilny. Tom II. Komentarz. Art. 353-626, Legalis 2022r., wyd. 3., kom. do art. 472, nb 2.

[24] Tak m.in. *M. Gutowski*, w: *M. Gutowski* (red.), Kodeks cywilny. Tom II. Komentarz. Art. 353-626, Legalis 2022 r., kom. do art. 472 KC, nb 4.Podobnie także *W. Borysiak*, w: *K. Osajda* (red. serii), W. *Borysiak* (red. tomu), Kodeks cywilny. Komentarz, Legalis 2022 r., wyd. 30, kom. do art. 472, nb 26.

[25] W tym tonie m.in. wyr. SN z 11.5.2005 r., III CK 522/04 oraz wyr. SA w Katowicach z 25.7.2013 r., V ACa 472/12. Por. także *M. Gutowski*, op. cit., nb 5.

[26] Por. przykłady zachowań płatników przytaczane przez *T. Czecha*, w: *K. Osajda* (red. serii), *J. Dybiński* (red. tomu), Ustawa o usługach płatniczych. Komentarz, Legalis 2022 r., wyd. 1, kom. do art. 42, nb 30–31.

[27] Co, rzecz jasna, odbywa się na ryzyko tego dostawcy. Dostawca ryzykuje bowiem naruszeniem umowy oraz naruszeniem przepisów prawa. Nie jest to jednak sytuacja jakkolwiek wyjątkowa, w porównaniu do typowych kontraktowych stosunków zobowiązaniowych.

oceny, czy doszło do umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia obowiązków użytkownika może dokonać wyłącznie sąd[28]. Ocena dokonana przez sąd jest oczywiście wiążąca w sytuacji spornej pomiędzy użytkownikiem i dostawcą. Dopiero na tym etapie możliwe jest ewentualne uznanie kwalifikacji naruszenia obowiązków użytkownika dokonanej przez dostawcę usług płatniczych za błędną. Jednak **każda ze stron umowy uprawniona jest do oceny wykonania zobowiązania przez drugą ze stron.** Jest to naturalny element stosunków zobowiązaniowych, także w obrocie konsumenckim. Podobnie, nieuzasadnione jest w naszej ocenie stanowisko organów konsumenckich[29], zgodnie z którym dostawca zawsze ma obowiązek dokonać zwrotu na rzecz użytkownika w przypadku zgłoszenia transakcji nieautoryzowanej (za wyjątkiem upływu terminu zawitego lub podejrzenia oszustwa ze strony płatnika) i jedynie na zasadzie niejako „regresowej" mógłby następnie dochodzić od użytkownika zapłaty w ramach postępowania sądowego (jeżeli uważa, że zwrot był nienależny). Przepisy art. 46 ust. 2-6 UUP określają materialnoprawne ramy rozkładu ciężaru finansowego między dostawcą i użytkownikiem w przypadku wystąpienia transakcji nieautoryzowanych. Skoro tak, to zarówno dostawca i użytkownik mogą dokonać subsumpcji określonego stanu faktycznego i ocenić, która ze stron i w jakim zakresie ponosi ciężar finansowy danej transakcji nieautoryzowanej. Trudno byłoby natomiast zaakceptować wniosek, że skoro dostawca usług płatniczych nie dopatruje się swojej odpowiedzialności w konkretnym przypadku (np. przypisując użytkownikowi rażące niedbalstwo), to mimo wszystko jest niejako zmuszony przez prawodawcę do spełnienia na rzecz użytkownika świadczenia nienależnego (art. 410 KC). W myśl tej koncepcji, dostawca ten musiałby następnie dochodzić od użytkownika zwrotu tego nienależnego świadczenia w ramach postępowania sądowego. Na przyjęcie takiej konkluzji na pewno nie pozwala ani obecny kształt UUP, ani też założenie racjonalnego prawodawcy. UUP nie wprowadza w tym zakresie żadnych wyjątków od ogólnych zasad prawa zobowiązań. Gdyby zaś intencją prawodawcy faktycznie było to, aby dostawca w każdym przypadku był obowiązany dokonywać zwrotu kwoty transakcji na rzecz użytkownika – niezależnie od stopnia możliwych do przypisania mu zaniedbań – to należy przyjąć, że uczyniłby to wprost, czego wymaga konstytucyjna zasada ochrony swobody działalności gospodarczej (art. 22 Konstytucji). Zupełnie inną kwestią są natomiast przesłanki aktualizujące obowiązek zwrotu w tzw. terminie D+1 (art. 46 ust. 1 UUP), co szerzej analizowaliśmy w przywoływanej wcześniej analizie dla Warszawskiego Instytutu Bankowości.

VI. Przykłady nieprawidłowego zachowania użytkownika

39. Nie jest możliwe stworzenie katalogu zachowań użytkowników, które w każdym przypadku powinny być kwalifikowane jako rażące niedbalstwo. Ocena konkretnego zachowania musi być dokonywana przez pryzmat jej faktycznego i kontraktowego kontekstu – może się także zmieniać ze względu na omawianą wcześniej ewolucję modelu należycie starannego użytkownika.

40. Użyteczne wydaje się jednak podjęcie próby wyróżnienia grupy zachowań, z którymi wiązać można znaczne prawdopodobieństwo zasadności zaklasyfikowania ich jako przejawów rażącego niedbalstwa. Uważamy, iż uprawnione jest objęcie relewantnym zbiorem następujących zachowań:

[28] Por., m.in., stanowisko Prezesa UOKiK w sprawie interpretacji przepisów ustawy z 19 sierpnia 2011 r. o usługach płatniczych w zakresie dotyczącym nieautoryzowanych transakcji płatniczych z dnia 16 listopada 2022 r., opubl. na stronie UOKiK (https://uokik.gov.pl/download.php?plik=26783); dostęp 17 listopada 2022 r.), ss. 1 oraz 5.

[29] *Tamże.* W stanowisku tym wskazano, że: *„[p]odejrzenie dostawcy usług płatniczych, że płatnik doprowadził do nieautoryzowanej transakcji 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., nie stanowi przesłanki do odmowy zwrotu płatnikowi kwoty nieautoryzowanej transakcji. W takim przypadku dostawca usług płatniczych* ***może wystąpić względem płatnika z roszczeniem o zapłatę****. Jeżeli jednak płatnik nie zgadza się z oceną dostawcy usług płatniczych co do dopuszczenia się rażącego niedbalstwa, ostateczna ocena tych okoliczności (i tym samym odpowiedzialności płatnika za taką transakcję) powinna być dokonana przez sąd."*

Nr	Rodzaj instrumentu płatniczego	Przykłady zachowania rażąco niedbałego
1.	Karta płatnicza	Użytkownik pozostawia swoją kartę płatniczą w miejscu publicznym w sposób niezabezpieczony (np. w niezamkniętej szafce na siłowni, na stoliku w kawiarni). Następnie dochodzi do wykonania nisko kwotowych transakcji płatniczych przy użyciu tej karty. Użytkownik narusza wynikający z umowy ramowej obowiązek ostrożnościowy przechowywania karty płatniczej z należytą starannością.
2.	Karta płatnicza	Użytkownik otrzymuje e-mail z nieznanego adresu pocztowego. W treści otrzymanej wiadomości użytkownik jest proszony o podanie numeru karty płatniczej, daty jej ważności, numeru CVV/CVC oraz dodatkowych danych uwierzytelniających, aby otrzymać wypłatę wysokiej wygranej w loterii. Użytkownik nie zachowuje ostrożności co do pochodzenia ww. wiadomości, wierzy w wygraną, której nie powinien się spodziewać i w odpowiedzi przekazuje wszystkie żądane informacje. W efekcie dochodzi do użycia karty płatniczej użytkownika poprzez wykonanie transakcji zdalnej (online). Użytkownik narusza wynikający z umowy ramowej obowiązek ostrożnościowy niepodawania chronionych danych (danych uwierzytelniających) osobom trzecim.
3.	Karta płatnicza	Użytkownik otrzymuje e-mail lub wiadomość z komunikatora internetowego (np. Messenger, Whatsapp) i używa linka prowadzącego do fałszywej strony imitującej stronę banku. Na tej stronie użytkownik podaje pełne dane uwierzytelniające swojej karty płatniczej (imię i nazwisko, numer karty, data ważności, numer CVV/CVC). Następnie dochodzi do użycia przekazanych danych przez nieuprawnioną osobę trzecią w celu zainicjowania procesu dodania („stokenizowania") karty płatniczej w aplikacji typu *wallet* (np. Google Pay, Apple Pay), zainstalowanej na urządzeniu mobilnym oszusta. Ukończenie tego procesu zabezpieczone jest dodatkowym uwierzytelnieniem, np. wymaga podania jednorazowego kodu (OTP) przesłanego na urządzenie użytkownika przez SMS lub z wykorzystaniem IVR. W komunikacie przekazującym kod aktywacyjny bank informuje użytkownika, że jest to kod umożliwiający dodanie karty płatniczej do innego urządzenia i jednocześnie wzywa do zachowania ostrożności. Użytkownik ignoruje ostrzeżenie i przekazuje kod na fałszywej stronie. W efekcie dochodzi do umożliwienia oszustowi dokonywania płatności kartą wirtualną (tokenem karty płatniczej użytkownika)[30]. Użytkownik narusza wynikający z umowy ramowej obowiązek ostrożnościowy niepodawania chronionych danych (danych uwierzytelniających) osobom trzecim. Użytkownik nie dochowuje także ogólnej staranności związanej z bezpiecznym korzystaniem z instrumentu płatniczego, w tym ignoruje komunikaty przesyłane przez bank oraz nie weryfikuje, czy domena strony internetowej jest taka, z jakiej z reguły loguje się do bankowości internetowej. Użytkownik nie weryfikuje także, czy strona internetowa zabezpieczona jest protokołem SSL.

[30] Nie odnosimy się tutaj do problematyki konieczności zabezpieczenia niektórych transakcji kartą płatniczą SCA.

Nr	Rodzaj instrumentu płatniczego	Przykłady zachowania rażąco niedbałego
4.	Bankowość internetowa	Użytkownik sprzedaje rzecz na platformie internetowej typu *marketplace*. Osoba, która jest pozornie zainteresowana zakupem rzeczy od użytkownika, przekazuje mu link rzekomo umożliwiający otrzymanie płatności z tytułu sprzedaży, gdzie użytkownik wybiera swój bank i podaje swoje dane dostępowe do systemu bankowości internetowej. Według informacji przekazanych przez oszusta, podanie tych danych ma umożliwić użytkownikowi otrzymanie transakcji (ceny) od osoby zainteresowanej zakupem. Następnie oszust dalej wprowadza użytkownika w błąd i informuje go o konieczności potwierdzenia przyjęcia transakcji kodem otrzymanym od banku w SMS. W rzeczywistości oszust używa przekazanych danych dostępowych do systemu bankowości internetowej w celu samodzielnego zalogowania się na konto użytkownika i zlecenia przelewu z jego konta, który dodatkowo potwierdza kodem z SMS przekazanym mu przez użytkownika. Użytkownik narusza wynikający z regulaminu banku obowiązek ostrożnościowy nieotwierania linków przesłanych przez nieznanych adresatów oraz obowiązek nieprzekazywania danych dostępowych osobom trzecim. Użytkownik dodatkowo ignoruje treść SMS-a pochodzącego od banku, który zawiera kod uwierzytelniający, w którym wskazano, że użytkownik powinien użyć tego kodu do uwierzytelnienia transakcji wychodzącej w określonej kwocie, a nie akceptacji transakcji przychodzącej (zignorowanie treści wiadomości). Użytkownik nie weryfikuje także, czy domena strony internetowej jest taka, z jakiej z reguły loguje się do bankowości internetowej.
5.	Bankowość internetowa	Użytkownik przechowuje dane dostępowe do systemu bankowości elektronicznej zapisane na kartce przyklejonej do swojego laptopa. Dochodzi do ich wykradnięcia / podpatrzenia w miejscu publicznym, gdzie użytkownik używał swojego komputera. Za pomocą pozyskanych danych oszustowi udaje się uzyskać dostęp do informacji o adresie e-mail użytkownika, na który następnie przesyła fałszywą wiadomość o konieczności uiszczenia zaległej opłaty za przesyłkę kurierską czy opłacenia zaległego rachunku za prąd. Użytkownik używa linku przesłanego mu w wiadomości e-mail w celu dokonania zapłaty. W tym czasie oszust zleca (inicjuje) z jego rachunku transakcję polecenia przelewu. Użytkownik wpisuje we wskazanym miejscu kod uwierzytelniający z SMS-a otrzymanego od banku (którego oszust używa do uwierzytelnienia transakcji) lub samodzielnie potwierdza transakcję w aplikacji mobilnej. Dochodzi do zlecenia transakcji płatniczych z rachunku użytkownika. Użytkownik narusza obowiązek niepodawania danych uwierzytelniających osobom trzecim, a także ignoruje treść wiadomości SMS z kodem uwierzytelniającym lub treść komunikatu wyświetlanego przy potwierdzaniu transakcji w aplikacji mobilnej.
6.	Bankowość internetowa	Użytkownik otrzymuje e-mail z informacją o konieczności uiszczenia zaległej opłaty za przesyłkę kurierską czy opłacenia zaległego rachunku za prąd. Użytkownik używa linka prowadzącego do fałszywej strony imitującej stronę banku. Na tej stronie użytkownik podaje pełne dane uwierzytelniające do bankowości internetowej, o które jest proszony. W tym czasie – w oparciu o pozyskane dane – oszust zleca (inicjuje) z jego rachunku transakcję polecenia przelewu. Użytkownik wpisuje we wskazanym miejscu kod uwierzytelniający z SMS-a otrzymanego od banku (którego oszust używa do uwierzytelnienia transakcji). Użytkownik narusza obowiązek niepodawania danych uwierzytelniających osobom trzecim, a także ignoruje treść wiadomości SMS z kodem uwierzytelniającym lub treść komunikatu wyświetlanego przy potwierdzaniu transakcji w aplikacji mobilnej.

Nr	Rodzaj instrumentu płatniczego	Przykłady zachowania rażąco niedbałego
7.	Aplikacja lub urządzenie mobilne	Użytkownik pozostawia bez nadzoru swój smartfon z zainstalowaną aplikacją mobilną banku. Smartfon nie jest zabezpieczony. W notatkach w telefonie zapisana jest lista haseł do systemu bankowości elektronicznej (mobilnej). Osoba trzecia – za pomocą aplikacji mobilnej – zleca transakcje płatnicze. Użytkownik narusza wynikający z regulaminu banku obowiązek ostrożnościowy nieprzechowywania zapisanych haseł w urządzeniu mobilnym.
8.	Aplikacja lub urządzenie mobilne	Z użytkownikiem kontaktuje się telefonicznie osoba podająca się za pracownika banku, w którym użytkownik posiada rachunek, i przekonuje go, że powinien zainstalować ważne oprogramowanie (np. antywirusowe) na swoim komputerze lub urządzeniu mobilnym. W rzeczywistości dochodzi do zainstalowania oprogramowania do zdalnego sterowania urządzeniem użytkownika (zdalny pulpit). Aplikacja działa w tle, gdy użytkownik korzysta z aplikacji mobilnej swojego banku, co umożliwia podejrzenie oszustowi kodu PIN używanego do logowania do systemu banku[31]. W następstwie tych zdarzeń możliwe jest wykonywanie transakcji z rachunku użytkownika. Użytkownik narusza wynikający z regulaminu banku obowiązek ostrożnościowy niepodawania chronionych danych osobom trzecim oraz nieinstalowania nieznanego oprogramowania na urządzeniu mobilnym.
9.	Aplikacja lub urządzenie mobilne	Z użytkownikiem kontaktuje się telefonicznie osoba podająca się za pracownika banku lub policjanta (np. z numeru, na który nie da się oddzwonić) i przekonuje użytkownika, że powinien podać mu swoje indywidualne dane uwierzytelniające (powody w praktyce są różne). W międzyczasie osoba ta instaluje na swoim urządzeniu mobilnym aplikację banku, w którym użytkownik posiada rachunek. Wskutek zabiegów socjotechnicznych użytkownik przekazuje oszustowi kod z SMS-a przesłanego przez bank lub kod uzyskany na infolinii banku, który służy do uwierzytelnienia (zaufania) aplikacji banku na nowym urządzeniu mobilnym i powiązania go z rachunkiem użytkownika. SMS z kodem lub infolinia wyraźnie ostrzegają użytkownika, aby nikomu nie podawał uzyskiwanych kodów. Pomimo to, dzięki przekazanym przez użytkownika danym, oszust uzyskuje dostęp do rachunku użytkownika i dokonuje powiązania z nim nowej aplikacji. W następstwie tych zdarzeń dochodzi do wykonania transakcji z rachunku użytkownika. Użytkownik narusza wynikający z regulaminu banku obowiązek ostrożnościowy niepodawania chronionych danych osobom trzecim oraz ignoruje treść otrzymywanych od banku komunikatów, które informują o skutkach użycia przekazywanego użytkownikowi kodu uwierzytelniającego.

[31] Należy jednak zasygnalizować, że niekiedy bankowe aplikacje mobilne uniemożliwiają działanie w tle oprogramowania typu „zdalny pulpit", co może mieć wpływ na ocenę zachowania użytkownika w konkretnym przypadku.

Nr	Rodzaj instrumentu płatniczego	Przykłady zachowania rażąco niedbałego
10.	Aplikacja lub urządzenie mobilne	Z użytkownikiem telefonicznie kontaktuje się rzekomy przedstawiciel giełdy kryptowalut, za pomocą której użytkownik wcześniej inwestował. Oszust informuje klienta, że giełda chce dokonać na rzecz użytkownika zwrotu zdeponowanych tam środków. W tym celu oszust namawia użytkownika, że wyśle do użytkownika link aktywacyjny, który pozwoli zrealizować płatność. Kliknięcie w link powoduje uruchomienie procesu instalacyjnego aplikacji zdalnego pulpitu, która umożliwia zdalny dostęp do urządzenia użytkownika (np. telefonu) przez osobę trzecią. Proces instalacji ww. aplikacji poprzedzony jest komunikatem informującym o charakterze tej aplikacji. Pomimo tego użytkownik dokonuje instalacji. Następnie użytkownik proszony jest o podanie numeru rachunku bankowego, aby giełda kryptowalut dokonała zwrotu środków. Użytkownik nie zna na pamięć numeru rachunku i w tym celu loguje się do rachunku z wykorzystaniem aplikacji mobilnej. Logowanie odbywa się poprzez podanie PIN. W tle tych czynności działa aplikacja zdalnego pulpitu, która pozwala oszustowi na podgląd danych uwierzytelniających (PIN)[32]. Po zalogowaniu się do aplikacji mobilnej oszust przejmuje kontrolę nad urządzeniem użytkownika i składa zlecenia poleceń przelewów. Następnie wykorzystuje PIN użytkownika (uzyskany wskutek podglądu) do zatwierdzenia zleceń płatniczych. Użytkownik narusza wynikający z regulaminu banku obowiązek ostrożnościowy niepodawania chronionych danych osobom trzecim oraz nieinstalowania nieznanego oprogramowania na swoich urządzeniach mobilnych.

41. Należy w szczególności zwrócić uwagę, że omawiane zachowania i nieprawidłowości nie są zjawiskami nowymi. Są to sytuacje, które w praktyce obrotu powtarzają się dosyć regularnie – i to na przestrzeni co najmniej kilku ostatnich lat. **Zachowań tych nie można więc mierzyć miarą statyczną.** Jeżeli nawet niektóre z tych zachowań nie byłyby uznane za rażąco niedbałe jeszcze parę lat temu, to nie znaczy, że jest tak nadal. **Należy oczekiwać od użytkowników korzystających z ugruntowanych już w praktyce instrumentów płatniczych, że ich świadomość i ostrożność będą zwiększać się wraz z upływem czasu[33].** Przykładowo, aplikacje bankowości mobilnej lub zdigitalizowane (wirtualne) karty płatnicze stanowiły jedynie wycinek instrumentów stosowanych w obrocie płatniczym jeszcze w pierwszej dekadzie XXI wieku. Nic więc dziwnego, że w tym okresie użytkownicy mogli nie zdawać sobie sprawy z pożądanych zasad przechowywania danych uwierzytelniających do takich aplikacji, czy też z niebezpieczeństw związanych z umożliwieniem przez użytkownika digitalizacji karty na urządzeniu osoby trzeciej. Trudno byłoby jednak przyjąć, że zasady korzystania z takich instrumentów są obecnie tak samo obce, jak wtedy.

42. Wskazać należy również, że stwierdzenie rażącego niedbalstwa nie prowadzi do obciążenia użytkownika za nieautoryzowaną transakcję, jeżeli dla jej zainicjowania dostawca usług płatniczych powinien był wymagać SCA, a tego nie zrobił (art. 46 ust. 4a UUP). Na przykład użycie skradzionej karty (pierwszy ze scenariuszy opisanych powyżej) do zainicjowania transakcji zdalnej, która została wykonana przez dostawcę z naruszeniem wymogu SCA, nie powoduje obciążenia użytkownika jej skutkami.

[32] Uwaga jak wyżej – niekiedy bankowe aplikacje mobilne uniemożliwiają działanie w tle oprogramowania typu „zdalny pulpit", co może mieć wpływ na ocenę zachowania użytkownika w konkretnym przypadku.

[33] Podobnie w odniesieniu do wzorca należytej staranności w stosunkach zobowiązaniowych *M. Safjan*, w: *K. Pietrzkowski* (red.), Kodeks cywilny. Tom I. Komentarz. Art. 1-449[10], Legalis 2018 r., wyd. 9, kom. do art. 355, nb 4. Autor ten wskazuje, że zobiektywizowane kryteria należytej staranności są kategorią dynamiczną i ewoluują wraz ze zmianami cywilizacyjnymi oraz rosnącymi oczekiwaniami uczestników obrotu. Stopień wymagań w odniesieniu do staranności jest podporządkowany w wielu dziedzinach kryteriom wynikającym z rozwoju nowoczesnej technologii, coraz powszechniejszej dostępności środków komunikacji i informacji, czy znacząco zwiększającym się wymaganiom współczesnej klienteli na nowoczesnym, konkurencyjnym rynku. Proces zmiany i ewolucji zachodzi więc obecnie znacznie szybciej niż jeszcze kilkanaście lat temu. Oznacza to, że te same miary staranności, które jeszcze niedawno odpowiadały w pełni przyjętym powszechnie wymaganiom są dzisiaj pozbawione aktualności i stały się anachroniczne.

VII. Aktualne orzecznictwo

43. Dokonanie oceny stanu spraw związanych z transakcjami nieautoryzowanymi wymaga nie tylko sięgnięcia do praktyki rynkowej, ale także zbadania orzecznictwa.

44. Przeprowadzony przez nas przegląd dorobku judykatury objął 57 wyroków rozstrzygających spory dotyczące odpowiedzialności za transakcje nieautoryzowane, które wydane zostały w latach 2016-2022. Większość spośród nich zapadła na poziomie sądów okręgowych i rejonowych. Brak jest w tym zakresie relewantnych orzeczeń Sądu Najwyższego.

45. Orzeczenia uwzględnione w ramach przeprowadzonego przeglądu zostały wyszukane w Portalu Orzeczeń Sądów Powszechnych oraz w Systemie Informacji Prawnej LEX[34], a także poprzez przegląd orzeczeń zaklasyfikowanych jako „powiązane" z art. 42 i 46 UUP w Systemie Informacji Prawnej LEX. Zidentyfikowane orzeczenia stanowią wszystkie orzeczenia, które udało nam się ustalić w oparciu o przedstawioną powyżej metodykę. Przegląd nie obejmował natomiast orzeczeń oznaczonych w Portalu Orzeczeń Sądów Powszechnych jako nieprawomocne oraz rozstrzygnięć zapadłych w sprawach dotyczących odpowiedzialności za wykonywanie transakcji płatniczych, w których sąd nie analizował kwestii spełnienia przesłanek z art. 46 ust. 3 UUP. Dodatkowo, 9 orzeczeń spośród przywoływanych w niniejszym opracowaniu, zostało przez nas pozyskane w ramach prac grupy roboczej dotyczącej transakcji nieautoryzowanych przy Związku Banków Polskich.

46. W licznych orzeczeniach[35] sądy nie uznały za zasadne przypisania **użytkownikom rażącego niedbalstwa i uznały, iż ponoszą oni** jedynie ograniczoną odpowiedzialność za transakcje nieautoryzowane. W uzasadnieniach rozstrzygnięć idących w tym kierunku akcentowano fakt, że banki są podmiotami profesjonalnymi i wyspecjalizowanymi oraz podkreślano znaczenie ciążących na nich obowiązków w zakresie zapewnienia zabezpieczeń systemów bankowości elektronicznej[36].

47. Na szczególną uwagę zasługują sprawy, w których zdarzeniem powodującym uszczerbek jest wyłudzenie podstępem od użytkowników danych uwierzytelniających. Sądy niekiedy (choć stosunkowo rzadko) nie kwalifikują zachowań użytkowników, którzy padli ofiarą takich podstępów, jako rażącego niedbalstwa[37]. Okolicznością, którą niekiedy traktuje się jako wystarczające usprawiedliwienie użytkownika i która jednocześnie wyłącza zasadność przypisania mu rażącego niedbalstwa, jest w szczególności „profesjonalny", wysoce przebiegły charakter oszustwa. W judykaturze przyjmowano, że w takich przypadkach przeciętny użytkownik nie jest w stanie uchronić się przed mechanizmami i skutkami takiego oszukańczego działania[38].

48. Wyraźne zmiany linii judykatury w ostatnich latach, a zwłaszcza w latach 2021-2022, zaobserwować można w sprawach, w których oszuści zdołali doprowadzić do dokonania transakcji nieautoryzowanych dzięki zastosowaniu taktyki ***phishingu***[39]. **W najnowszym orzecznictwie zachowania użytkowników bywają w takich przypadkach uznawane za rażąco niedbałe.**

[34] Orzeczenia te zostały wyszukane za pomocą słowa kluczowego „autoryzacja".

[35] Por. np. wyr. SA w Białymstoku z dnia 3 października 2019 r., I ACa 228; wyr. SA w Białymstoku z dnia 2 marca 2020 r., sygn. I AGa 4/19; wyr. SA w Łodzi z dnia 10 marca 2017 r., sygn. I ACa 1174/16; wyr. SA w Łodzi z dnia 17 stycznia 2020 r., sygn. I ACa 1511/18; wyr. SO w Gliwicach z dnia 23 maja 2017 r., sygn. II C 421/16; wyr. SR w Gliwicach z dnia 18 lipca 2016 r., sygn. I C 2524/14; wyr. SO w Łodzi z dnia 2 maja 2017 r., sygn. III Ca 43/17; wyr. SO w Łodzi z dnia 4 września 2017 r., sygn. III Ca 611/17; wyr. SO w Łodzi z dnia 30 października 2018 r., sygn. II C 73/16; wyr. SO w Łodzi z dnia 3 stycznia 2017 r., sygn. III Ca 1101/16; wyr. SO w Łodzi z dnia 11 stycznia 2017 r., sygn. III Ca 1401/16; wyr. SO w Bielsku Białej z dnia 6 grudnia 2018 r., sygn. I C 338/17; wyr. SO w Warszawie z dnia 12 maja 2018 r., sygn. I C 566/17; wyr. SO w Poznaniu z dnia 24 września 2021, sygn. XV Ca 378/21; wyr. SO w Łodzi z dnia 31 lipca 2017 r., sygn. III Ca 716/17; wyr. SO w Łodzi z dnia 15 stycznia 2016 r., sygn. I C 307/15; wyr. SO w Krakowie z dnia 3 lipca 2018 r., sygn. II Ca 452/18; wyr. SO w Olsztynie z dnia 21 grudnia 2018 r., sygn. I C 55/18; wyr. SO w Warszawie z dnia 11 sierpnia 2021 r., sygn. XXVII Ca 1352/21; wyr. SR w Łodzi z dnia 7 września 2017 r., sygn. I C 249/16; wyr. SR Szczecin– Centrum z dnia 21 lutego 2022 r., sygn. I C 307/21; wyr. SR w Łodzi z dnia 14 czerwca 2016 r., sygn. I C 1024/14; wyr. SR w Łodzi z dnia 17 lutego 2021 r., sygn. VIII C 873/18; wyr. SR Poznań-Stare Miasto z dnia 8 grudnia 2021 r., sygn. I C 648/20; wyr. SR Łódź Śródmieście z dnia 2 stycznia 2017 r., sygn. III C 86/16.

[36] Por. np. wyr. SA w Warszawie z dnia 19 lipca 2018 r., sygn. I ACa 348/17, gdzie wskazano, że kilkukrotne próby zmian zabezpieczeń konta klientki, nieudane logowania i zmiany hasła nie wzbudziły podejrzeń banku, a powinny, zwłaszcza że IP komputera było inne niż to, z którego użytkownik zasadniczo dokonywał transakcji. W podobnym tonie wyr. SA w Białymstoku z dnia 5 kwietnia 2019 r., I AGa 176/18, a także wyr. SO w Warszawie z dnia 19 grudnia 2016 r., sygn. I C 229/15 oraz wyr. SR w Szczecinie z dnia 11 lutego 2019 r., sygn. XI GC 1962/18.

[37] Por. np. wyr. SA w Warszawie z dnia 24 maja 2018 r., sygn. VI ACa 217/17.

[38] Por. np. wyr. SO w Łodzi z dnia 18 kwietnia 2016 r., sygn. III Ca 24/16. W wyroku tym sąd wskazał, że nie można mówić o rażącym niedbalstwie w sytuacji, gdzie użytkownik padł ofiarą przestępstwa na tyle dobrze przygotowanego, że nie ustrzegło się przed nim wiele innych osób.

[39] W uproszczeniu można przyjąć, że *phishing* to oszustwo, które wykorzystuje metody socjotechniczne, za pomocą których przestępcy próbują oszukać użytkowników i spowodować, aby podjęli oni kroki zgodne z zamierzeniami tych przestępców. Chodzi tutaj często o sytuacje podszywania się oszustów pod spółki kurierskie, urzędy administracji, operatorów telekomunikacyjnych lub internetowych czy nawet pod same banki, aby za pomocą różnych technik (np. link w SMS albo link w wiadomości e-mail prowadzący do fałszywej strony) wyłudzić i przywłaszczyć dane uwierzytelniające do bankowości elektronicznej.

Tak kwalifikowane bywa m.in. nierozważne doprowadzanie do ujawniania poufnych danych uwierzytelniających, brak odczytywania komunikatów uwierzytelniających przesyłanych przez bank (np. w formie SMS)[40], przechowywanie instrumentu płatniczego w sposób niezabezpieczony[41], zaniechanie odpowiedniego informowania banku o podejrzeniach co do naruszenia bezpieczeństwa instrumentu płatniczego (np. podejrzeń dotyczących autentyczności strony bankowości internetowej)[42] czy też ignorowanie ogólnych kampanii informacyjnych prowadzonych przez banki[43].

49. Szczególnie interesujący jest wyrok Sądu Okręgowego w Gliwicach z 6 lipca 2022 r.[44]. W sprawie tej użytkownik za pomocą komunikatora internetowego prowadził korespondencję z nieznaną sobie osobą na temat sprzedaży butów dziecięcych na portalu internetowym. Oszust przekonał użytkownika do wysłania butów za pośrednictwem określonej usługi kurierskiej i twierdził, że użytkownik otrzyma potwierdzenie zamówienia oraz kod, z którym będzie mógł udać się do paczkomatu i włożyć paczkę do skrzynki. Użytkownik potwierdził zamówienie na formularzu, do którego przesłano mu link prowadzący do fałszywej strony internetowej. Na tej stronie użytkownik wpisał dane swojej karty kredytowej, a po otrzymaniu od banku wiadomości uwierzytelniającej o treści: „Wprowadź kod ****** aby potwierdzić aktywację karty nr... ******", wpisał ten kod i wysłał go. Nieznana osoba trzecia, która twierdziła, że jest zainteresowana kupnem butów, wykorzystała dane karty płatniczej i kod, ujawnione za pomocą fałszywej strony internetowej, w celu dodania karty płatniczej użytkownika w usłudze pozwalającej na zdigitalizowanie karty na urządzeniu mobilnym oszusta. Dodanie karty do nowego urządzenia umożliwiło oszustowi wykonywanie nią dalszych operacji, w tym wykonanie transakcji płatniczych w ciężar rachunku użytkownika.

50. Całokształt zachowania użytkownika sąd ocenił jako rażąco niedbały. W szczególności wskazał, że skorzystanie przez użytkownika z kodu SMS, potwierdzającego aktywację karty na urządzeniu mobilnym, **w sytuacji, gdy użytkownik już korzystał z tej usługi od dłuższego czasu i wiedział, jak przebiega procedura jej aktywowania**, wskazuje na rażące niedbalstwo, które doprowadziło do udostępnienia instrumentu płatniczego osobie nieuprawnionej[45].

51. Istotne dla praktyki obrotu są także nowsze orzeczenia zapadłe w sprawach, gdzie istotą oszustwa było nakłonienie użytkownika do instalacji programu pozwalającego na **zdalny dostęp do urządzenia** (tzw. zdalny pulpit, np. popularne programy AnyDesk czy TeamViewer). Chodzi tu o sytuacje, w których w wyniku zabiegów socjotechnicznych, oszust nakłonił użytkownika do zainstalowania na komputerze lub urządzeniu mobilnym (np. telefonie) programu pozwalającego na zdalny dostęp do niego (z reguły jest to oprogramowanie w pełni legalne), a następnie przy użyciu tego programu dochodzi do ujawnienia przez użytkownika oszustowi danych uwierzytelniających, przejęcia urządzenia przez oszusta i w efekcie doprowadzenia do nieautoryzowanych transakcji płatniczych. Tego typu przestępstwa dokonywane są relatywnie często. **Zachowania płatników, którzy wskutek niedochowania należytej ostrożności doprowadzają do instalacji oprogramowania zdalnego pulpitu i w efekcie do ujawnienia danych uwierzytelniających, bywają uznawane za daleko idące naruszenia postanowień umownych.** W przypadkach, w których towarzyszyły im jeszcze inne nieprawidłowości, sądy w kilku orzeczeniach przypisały użytkownikom rażące niedbalstwo.

52. Przykładowo, Sąd Rejonowy Katowice-Zachód w Katowicach (II C 752/21)[46] przypisał użytkownikowi rażące niedbalstwo. Uzasadnieniem tego ustalenia było to, że użytkownik nie zapoznawał się z kierowanymi do niego przez dostawcę ostrzeżeniami, choć **musiał zdawać sobie sprawę**, że zamieszczane są one po to, by ich lektura uchroniła go przed choćby nieumyślnym naruszeniem obowiązków umownych. W sprawie tej za przejaw rażącego niedbalstwa użytkownika uznano po pierwsze, zainstalowanie niezweryfikowanej i nieznanej aplikacji na polecenie

[40] Zob. np. wyr. SR w Świdnicy z dnia 4 października 2021 r., sygn. I C 538/20; wyr. SO w Łodzi z dnia 27 marca 2018 r., sygn. III Ca 51/18; wyr. SA w Warszawie z dnia 30 sierpnia 2018 r., sygn. VI ACa 509/17.
[41] Zob. np. wyr. SO w Warszawie z dnia 9 stycznia 2017 r., sygn. III C 918/15, gdzie wskazano, że użytkownik przechowywał komputer (z którego korzystał dla potrzeb bankowości internetowej) w pracy, a więc w miejscu, gdzie teoretycznie dostęp do niego miała nieograniczona liczba osób o tożsamości niemożliwej do zidentyfikowania.
[42] Zob. np. wyr. SO w Białymstoku z dnia 24 sierpnia 2017 r., sygn. II Ca 426/17; wyr. SO w Łodzi z dnia 26 kwietnia 2018 r., sygn. II C 342/17; wyr. SA w Warszawie z dnia 30 sierpnia 2018 r., sygn. VI ACa 509/17. Por. także wyr. SO we Wrocławiu z dnia 29 lipca 2013 r., sygn. I C 1476/12 – choć wyrok ten dotyczył oszustwa innego typu, którego przedmiotem były transakcje przy użyciu karty płatniczej.
[43] Zob. np. wyr. SR w Świdnicy z dnia 4 października 2021 r., sygn. I C 538/20 oraz wyr. SO w Warszawie z dnia 9 stycznia 2017 r., sygn. III C 918/15.
[44] Wyr. SO w Gliwicach z dnia 6 lipca 2022 r., sygn. III Ca 264/22.
[45] Można wskazać także na inne przykłady orzeczeń ws. phishingu, gdzie zachowanie użytkownika zakwalifikowano jako rażąco niedbałe. Por. m.in. wyr. SR w Białogardzie z dnia 14 lipca 2022 r., sygn. I C 517/20, czy też wyr. SO w Białymstoku z dnia 24 sierpnia 2017 r., sygn. II Ca 426/17.
[46] Wyr. SR Katowice-Zachód w Katowicach z dnia 13 lipca 2022 r., sygn. II C 752/21.

nieznanej osoby trzeciej, po drugie, podanie tej osobie w sposób bezrefleksyjny i nieuzasadniony wrażliwych danych umożliwiających w istocie nieograniczone możliwości ingerencji w jego rachunek bankowy oraz dokonywanie transakcji płatniczych, a po trzecie, niezweryfikowanie treści otrzymywanych od banku wiadomości SMS zawierających kody uwierzytelniające. Gdyby bowiem użytkownik zaznajomił się z ich treścią, zauważyłby, że są to kody służące dodaniu nowego urządzenia mobilnego do urządzeń zaufanych, co w dalszej kolejności umożliwiło składanie za jego pośrednictwem dyspozycji. Jako rażąco niedbałe sądy oceniły zachowania użytkowników także w nieco innych, lecz konstrukcyjnie zbliżonych stanach faktycznych[47].

53. Co istotne, oceniając stopień zawinienia po stronie użytkownika, w najnowszym orzecznictwie **sądy zwracają uwagę, że oczekiwany od użytkownika poziom staranności powinien być oceniany przez pryzmat obecnych realiów korzystania z instrumentów płatniczych**. Przykładowo, Sąd Rejonowy w Żyrardowie trafnie wskazał – przypisując użytkownikowi zachowanie rażąco niedbałe – że w rozpatrywanej tam sprawie użytkownik **nie wziął pod uwagę powszechnie pojawiających się w obrocie oszustw** polegających na podszywaniu się osób trzecich pod cudze numery telefonu[48]. Sąd wskazał, że *„oceniając zachowanie* [użytkownika] ***nie sposób także abstrahować od kontekstu społecznego i czasookresu****, w jakim miało miejsce* […] *zdarzenie. Sytuacja miała miejsce […] w okresie, kiedy w społeczeństwie* ***powszechne były informacje o różnorakich oszustwach*** *dokonywanych metodą na wnuczka, na policjanta, itp., w których przestępcy podszywali się pod inne osoby, celem wyłudzenia pieniędzy.* ***Inaczej można by oceniać zachowanie powoda w sytuacji, gdy tzw. oszustwa na zdalny pulpit byłyby zjawiskiem nowym****, o istnieniu których wielu użytkowników nawet nie zdawało sobie sprawy, a inaczej we wrześniu 2021 roku, kiedy pozwany bank już od kilku miesięcy prowadził kampanie* […] *dotyczące tego procederu, a zatem już wtedy było to zjawisko rozpowszechnione*".

54. Sąd, w uzasadnieniu badanego wyroku, wyraźnie zaznaczył też, że dokonując oceny stopnia winy użytkownika należy brać pod uwagę wzorzec zachowania należycie starannego użytkownika, jakiego oczekuje się nie tyle w obrocie płatniczym, co w obrocie zelektronizowanym. Przypisując użytkownikowi rażące niedbalstwo sąd wskazał, że **przeciętny użytkownik korzystający z urządzeń mobilnych ma świadomość tego**, że nie należy np. pobierać aplikacji, których przeznaczenie i legalność nie zostały zweryfikowane. Prawidłowa ocena zachowania użytkownika wymaga też, w ocenie sądu, aby wziąć pod uwagę, że użytkownik od kilku lat korzysta już z rozwiązań bankowości elektronicznej, a w efekcie można od niego oczekiwać **wyższego poziomu staranności** przy podejmowaniu decyzji związanych z dokonywaniem transakcji płatniczych[49].

55. Dokonana przez nas analiza orzecznictwa sądowego dotyczącego transakcji nieautoryzowanych pozwala na wyciągnięcie następujących kluczowych wniosków:

56. **Po pierwsze,** nie istnieje jednolita, w pełni ukształtowana linii orzecznicza dotycząca sposobu ujmowania przesłanki rażącego niedbalstwa na gruncie usług płatniczych.

57. **Po drugie,** wedle wielu zapadłych w ostatnich latach orzeczeń sądów zarówno pierwszej instancji, jak i sądów odwoławczych, przypisanie użytkownikowi rażącego niedbalstwa wymaga skrajnego naruszenia przez niego obowiązków związanych z korzystaniem z instrumentu płatniczego[50]. Niemniej, w ostatnim czasie (lata

[47] Por. wyr. SR w Suwałkach, sygn. I C 322/21, gdzie osoba podająca się za pracownika banku przekonała posiadaczkę rachunku bankowego do zainstalowania aplikacji o funkcjonalności zdalnego pulpitu, dzięki której możliwe było zlecanie przelewów z rachunku, uwierzytelnianych kolejnymi, przekazywanymi przez posiadaczkę rachunku kodami oraz wyr. SR w Żyrardowie z dnia 10 maja 2022 r., sygn. I C 718/21, gdzie podobnie, do wykonania wypłat czekami BLIK nastąpiło w wyniku zainstalowania aplikacji z funkcjonalnością zdalnego pulpitu. Por. także – na gruncie nieco innego stanu faktycznego – wyr. SA w Szczecinie z dnia 29 czerwca 2022 r., sygn. I ACa 97/22.

[48] Zob. wyr. SR w Żyrardowie z dnia 10 maja 2022 r., sygn. I C 718/21.

[49] *Tamże*. Por. np. wyr. Sądu Apelacyjnego w Szczecinie z dnia 29 czerwca 2022 r., sygn. I ACa 97/22.

[50] Por. wyr. SO w Łodzi z dnia 30 czerwca 2017 r., sygn. III Ca 716/17, gdzie płatnik po zalogowaniu do bankowości internetowej podał dodatkowy kod przesłany w wiadomości SMS w fałszywym oknie, które pojawiło się na stronie banku; wyr. SO w Krakowie z dnia 3 lipca 2018 r., sygn. II Ca 452/18, gdzie podczas logowania do bankowości internetowej płatnikowi wyświetlił się komunikat o konieczności odebrania poczty elektronicznej z linkiem prowadzącym do fałszywej stronie banku, na której płatnik się zalogował; por. także na gruncie podobnego stanu faktycznego – wyr. SO w Olsztynie z dnia 21 grudnia 2018 r., sygn. I C 55/18; wyr. SO w Łodzi z dnia 27 stycznia 2016 r., sygn. I C 1908/14, gdzie na skutek skorzystania z wyświetlającego się na stronie banku komunikatu zachęcającego użytkowników do pobrania dodatkowego oprogramowania antywirusowego płatnik zainstalował na telefonie komórkowym fałszywe oprogramowanie, które przekierowywało wiadomości kierowane na jego numer telefonu na inny numer; por. także na gruncie podobnego stanu faktycznego – wyr. SO w Warszawie z dnia 23 listopada 2017 r., sygn. I C 1016/15, gdzie zainstalowane przez płatnika fałszywe oprogramowanie antywirusowe wykradło dane dostępowe do rachunku. We wszystkich tych przypadkach nie stwierdzono rażącego niedbalstwa użytkownika.

2018–2022) zaczęły pojawiać się rozstrzygnięcia, w których podniesiono standard oczekiwań stawianych użytkownikom usług płatniczych[51].

58. **Po trzecie**, sprawy, w których sądy szczegółowo badają stopień zawinienia użytkownika usług płatniczych w kontekście transakcji nieautoryzowanych, w tym przez pryzmat naruszenia obowiązków nałożonych na niego w konkretnej umowie ramowej, ciągle są rzadkie. W ostatnich latach zapadło jednak kilka rozstrzygnięć, w których sądy szczegółowo zbadały zachowanie użytkownika na wskazanej płaszczyźnie [52].

59. **Po czwarte**, od kilku lat judykatura wydaje się nieco bardziej uwrażliwiona na potrzebę brania pod uwagę praktycznych aspektów bezpieczeństwa korzystania z instrumentów płatniczych. Obecnie sądy częściej traktują zasady korzystania z instrumentu płatniczego jako kategorię dynamiczną, zmienną w czasie i podlegającą ciągłej ewolucji oraz zależną od typu instrumentu płatniczego. Zachowania użytkowników, które wcześniej nie były rozpatrywane w kategoriach rażącego niedbalstwa, wraz ze stopniowym rozwojem usług płatniczych i elektronizacją obrotu, zaczęły być inaczej postrzegane przez sądy[53].

[51] Por. wyr. SA w Warszawie z dnia 30 sierpnia 2018 r., sygn. VI ACa 509/17; wyr. SA w Warszawie z dnia 30 sierpnia 2018 r., sygn. VI ACa 509/17; wyr. SO w Łodzi z dnia 27 marca 2018 r., sygn. III Ca 51/18; wyr. SO w Warszawie z dnia 9 stycznia 2017 r., sygn. III C 918/15; wyr. SO w Białymstoku z dnia 24 sierpnia 2017 r., sygn. II Ca 426/17; wyr. SO w Łodzi z dnia 26 kwietnia 2018 r., sygn. II C 342/17; wyr. SO w Gliwicach z dnia 6 lipca 2022 r., sygn. III Ca 264/22; Wyr. SR Katowice-Zachód w Katowicach z dnia 13 lipca 2022 r., sygn. II C 752/21; wyr. SR w Białogardzie z dnia 14 lipca 2022 r., sygn. I C 517/20; wyr. SR w Suwałkach, sygn. I C 322/21; wyr. SR w Żyrardowie z dnia 10 maja 2022 r., sygn. I C 718/21; wyr. SR w Świdnicy z dnia 4 października 2021 r., sygn. I C 538/20; wyr. SR w Świdnicy z dnia 4 października 2021 r., sygn. I C 538/20.

[52] Por. wyr. SA w Białymstoku z dnia 5 kwietnia 2019 r., sygn. I AGa 176/18; wyr. SO w Białymstoku z dnia 24 sierpnia 2017 r., II Ca 426/17; wyr. SO w Łodzi z dnia 26 kwietnia 2018 r., II C 342/17; wyr. SO w Gliwicach z dnia 6 lipca 2022 r., sygn. III Ca 264/22; wyr. SO w Warszawie z dnia 12 maja 2018 r., sygn. I C 566/17; wyr. SO w Łodzi z dnia 30 czerwca 2017 r., sygn. III Ca 716/17.

[53] Por. w szczególności wyr. SO w Gliwicach z dnia 6 lipca 2022 r., sygn. III Ca 264/22 oraz wyr. wyr. SR w Żyrardowie z dnia 10 maja 2022 r., sygn. I C 718/21 (omówione powyżej). Zob. także wyr. SR w Białogardzie z dnia 14 lipca 2022 r., sygn. I C 517/20, który wskazał m.in., że: *„[d]la każdego klienta banku korzystającego z instrumentu płatniczego w szczególności w ramach bankowości elektronicznej **powinno być oczywiste**, że zabezpieczenia indywidualne trzeba chronić przed dostępem osób trzecich (czy to spokrewnionych, czy obcych), bo ich udostępnienie ułatwia oczywiście innym dostęp do środków zgromadzonych na rachunku”* oraz w odniesieniu do znaczenia kodów uwierzytelniających, że; *„**[p]owszechnie wiadomo**, że kody te mogą służyć do płatności, ale również np. zmiany danych dostępowych (numeru telefonu klienta w bazie banku), zmiany limitu operacji płatniczych, składania wniosku o produkt bankowy itp.”*. Por. także wyr. SR Katowice-Zachód w Katowicach z dnia 13 lipca 2022 r., sygn. II C 752/21, który wskazał, że: *„[d]la każdego klienta banku korzystającego z instrumentu płatniczego **oczywiste winno być** więc, że indywidualne zabezpieczenia tego instrumentu muszą być chronione ze szczególną starannością przed dostępem osób trzecich, gdyż ich udostępnienie w znacznym stopniu ułatwia innym dostęp do funduszy zgromadzonych na rachunku”* oraz *„**przesłanie kodu winno uświadomić mu*** [użytkownikowi – przyp. aut.*], że ktoś zamierza dokonać transakcji bez jego zgody i wiedzy albo też – o ile jest mu to wiadome, ale osoba trzecia wprowadziła go w błąd co do rodzaju czynności wymagającej wprowadzenia kodu pozwolić mu na stwierdzenie, że w rzeczywistości wprowadzenie kodu spowoduje zatwierdzenie innego rodzaju dyspozycji”* oraz *„**banki powszechnie starają się uprzedzić** swoich klientów o podejmowanych nielegalnie próbach wyłudzenia indywidualnych zabezpieczeń instrumentów płatniczych, wskazując wprost, z jakimi działaniami mogą się zetknąć i jakich zachowań powinni unikać. Informacje takie zamieszczane są zwykle na stronach internetowych, z których klienci korzystają przy posługiwaniu się instrumentami płatniczymi, niejednokrotnie w ten sposób, że **nie jest możliwe pominięcie tej informacji** przed przystąpieniem do dalszych czynności na tej stronie”*.

VIII. Podsumowanie

60. Złożoność stanów faktycznych w zakresie transakcji nieautoryzowanych, jak również wysoce wyspecjalizowany charakter tej problematyki niewątpliwie stanowią wyzwanie nie tylko dla samych uczestników rynku (dostawców i użytkowników), ale także dla doktryny prawniczej i orzecznictwa. **Nie powinno jednak budzić wątpliwości, że z biegiem lat kluczowa rola w kształtowaniu właściwej praktyki rynkowej przypadać będzie właśnie sądownictwu.** Sprawy dotyczące transakcji nieautoryzowanych są z natury rzeczy podatne na spór. Interesy dostawców i użytkowników są w takich przypadkach rozbieżne, a często wysokie kwoty powstałych strat nie sprzyjają polubownemu rozstrzygania sporów. Dostrzegł to już sam prawodawca wprowadzając w ramach UUP szczególne zasady dowodowe oraz szczególne reguły odpowiedzialności, o czym pisaliśmy w poprzedniej analizie.

61. Z tego właśnie względu należy podjąć wszelkie starania, aby nieustannie zwiększać poziom bezpieczeństwa usług płatniczych (co jest zadaniem dostawców usług płatniczych), zwiększać czujność i ostrożność w zakresie korzystania z instrumentów płatniczych (co jest zadaniem użytkowników), a także właściwie rozstrzygać sytuacje graniczne, gdzie trudno jest jednoznacznie przesądzić o zwykłym lub rażącym niedbalstwie po stronie użytkownika usług płatniczych w przypadku wystąpienia transakcji nieautoryzowanych.

62. Zdarza się, że w jednej i tej samej sprawie, sąd kwalifikuje określoną transakcję jako transakcję autoryzowaną (art. 40 ust. 1 UUP) i jednocześnie jako transakcję, której powodem wystąpienia było rażące niedbalstwo klienta w przestrzeganiu zasad bezpieczeństwa (art. 46 ust. 3 UUP)[54]. Tymczasem, **jedna i ta sama transakcja nie może być jednocześnie autoryzowana, jak i nieautoryzowana w wyniku rażąco niedbałego naruszenia przez użytkownika ciążących na nim obowiązków.**

63. Dokonując oceny, czy zachowanie użytkownika w konkretnej sprawie cechuje niedbalstwo rażące czy zwykłe, należy brać pod uwagę nie tylko obowiązki wynikające z przepisów prawa, ale także ich konkretyzację w postaci zasad używania instrumentów płatniczych wynikających z **zawartej między stronami umowy ramowej (art. 42 ust. 1 pkt 1 UUP).**

64. Dokonując oceny, czy zachowanie użytkownika w konkretnej sprawie cechuje niedbalstwo rażące czy zwykłe, należy pamiętać, że oczekiwany od użytkowników poziom staranności jest kategorią w pewnym stopniu dynamiczną. **Inaczej powinny być więc oceniane zachowania w przypadku nowych oszustw i zagrożeń, a inaczej w przypadku oszustw i zagrożeń od dłuższego czasu znanych już należycie starannym użytkownikom.**

65. Ocena zachowania użytkownika jako prawidłowego, niedbałego lub rażąco niedbałego nie powinna sprowadzać się tylko do weryfikacji stanu wykonania umowy ramowej. Należy także wziąć pod uwagę inne okoliczności towarzyszące zasadom korzystania z instrumentów płatniczych wydawanych przez określonego dostawcę. **Należy w szczególności uwzględniać kontekst społeczny i czasowy, w jakim określone zdarzenie miało miejsce, to, czy informacje o określonych praktykach oszukańczych były rozpowszechnione w takim stopniu, że ich posiadania można było rozsądnie wymagać od przeciętnego użytkownika.**

66. Ocena zachowania użytkownika jako prawidłowego, niedbałego lub rażąco niedbałego powinna być przeprowadzana w oparciu o konkretne stosunki kontraktowe (umowy o usługi płatnicze). Na gruncie tych stosunków wzorzec należytej staranności, którego oczekuje się od użytkownika (płatnika), ma charakter zobiektywizowany, zewnętrzny i abstrakcyjny. W tym zakresie brak jest szczególnych zasad odróżniających regulację usług płatniczych od ogólnych reguł zobowiązaniowych.

[54] Przykładowo SR w Świdnicy w wyr. z dnia 4 października 2021 r., I C 538/20 wskazał, że użytkownik „mechanicznie autoryzował polecenie przelewu" i jednocześnie, że zachowanie płatnika świadczy o rażącym niedbalstwie tego użytkownika i stanowi naruszenie zobowiązania klienta do zachowania swoich danych w tajemnicy.

Raport przygotowany na zlecenie Fundacji
Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY