Fundacja Dobre Państwo

Warszawa - Poznań, dnia 3 marca 2025 r.

**Fundacja Dobre Państwo**

reprezentowana przez:
Witolda Solskiego
Katarzynę Kosakowską
działających na rzecz:
Kancelarii Doradczej
Solski i Partnerzy sp. z o.o.



**Pan**
**dr Andrzej Duda**
**Prezydent RP**
**w miejscu**

## PETYCJA

Na podstawie art. 63 Konstytucji RP i art. 2 art. 2 ust. 3 Ustawy o petycjach wnosimy petycję o podjęcie działań w celu wniesienia pod obrady Parlamentu projektu zmian legislacyjnych, których celem będzie uniemożliwienie okradania klientów w Polsce metodą B , wobec obciążania przez banki odpowiedzialnością za taki stan rzeczy klientów i obojętności instytucji powołanych do nadzoru nad rynkiem bankowym, w tym Komisji Nadzoru Finansowego, Narodowego Banku Polskiego oraz Związku Banków Polskich.

Proponowana przez nas zmiana polegać by miała na nadaniu art. 45 ust. 2 ustawy z dnia z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j: Dz.U.2024.30 z późn. zm.) następującego brzmienia:

Art. 45.2. Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego, ***w szczególności jeśli użytkownik niezwłocznie po użyciu środka płatniczego zgłosił reklamację,*** nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana albo że płatnik umyślnie albo wskutek rażącego niedbalstwa doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie albo wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42. Ciężar udowodnienia tych okoliczności spoczywa na dostawcy.

W.S.

[1] Rejestr podmiotów wykonujących zawodową działalność lobbingową prowadzony przez MSWiA

## UZASADNIENIE

B może wyczyścić Tobie konto w mig. Masz to jak w banku, że Ciebie też zechcą oszukać, lub okraść, a Państwo nie wiele pomoże.

Kochani, uzasadnienie zaczynamy od wyjaśnienia. Dokumenty drukujemy czcionką garamond, rozmiar 14, interlinia 1,15, tekst wyjustowany do prawa i lewa. Nie stosujemy pustych wersów. Każda linia jest zadrukowana. W stopce jest adres internetowy Fundacji Dobre Państwo oraz numer strony. Nie bierzemy odpowiedzialności za przesłanianie przez urzędnika organu fragmentów skanowanych materiałów. Na pierwszej stronie są pełne dane Petytora oraz data dokumentu. Nie znamy przyczyny i celu ingerowania w treść Petycji, której dopuszczają się urzędnicy. Przepraszamy za niedogodności poznawania merytoryki.

Oszustwo na B to metoda wyłudzenia pieniędzy polegająca na wykorzystaniu popularnego systemu płatności mobilnych B , w połączeniu z podszywaniem się pod zaufaną osobę lub instytucję. Mechanizm działania przestępców jest zazwyczaj dwuetapowy. Po pierwsze, oszust przejmuje kontrolę nad kontem ofiary w mediach społecznościowych lub kontaktuje się z nią, podszywając się pod bliską osobę albo kontrahenta. Następnie, za pośrednictwem komunikatora internetowego (np. M ) lub telefonu, przestępca prosi o wygenerowanie i podanie kodu B , tłumacząc to nagłą potrzebą finansową (np. awarią karty płatniczej, pilnym zakupem lub innym dramatycznym zdarzeniem). Osoba przekonana, że pomaga znajomemu, podaje sześciocyfrowy kod, nieświadoma, że w rzeczywistości trafia on do oszusta. Po uzyskaniu kodu sprawca natychmiast wykorzystuje go do wypłaty gotówki z bankomatu lub dokonania płatności. Środki znikają z konta ofiary w ciągu sekund.

Jednym z najczęstszych wariantów tego oszustwa jest podszycie się pod znajomego potrzebującego pilnie pieniędzy. Przestępcy włamują się na konto ofiary na F lub innym portalu społecznościowym i rozsyłają do jej znajomych wiadomości z prośbą o szybką pomoc finansową. Wykorzystują przy tym psychologiczne mechanizmy manipulacji: tworzą atmosferę nagłego kryzysu i presji czasu, apelują do empatii i zaufania między bliskimi osobami.

Ofiary często działają odruchowo, chcąc pomóc rzekomo potrzebującemu przyjacielowi czy krewnemu, co osłabia ich czujność. Innym wariantem jest oszustwo „na kupującego". Przestępcy odpowiadają na ogłoszenia sprzedaży (np. na portalach typu O lub F M ) i pod pretekstem uregulowania zapłaty proszą sprzedawcę o podanie kodu B lub kliknięcie w fałszywy link. Często posługują

się zautomatyzowanymi botami internetowymi, które masowo wysyłają wiadomości do sprzedawców tuż po publikacji ogłoszenia. W rzeczywistości kod B służy im do wypłaty pieniędzy z konta sprzedającego, który mylnie sądzi, że umożliwia odbiór zapłaty. Podobnie oszuści potrafią dzwonić do ofiar, podszywając się pod konsultanta platformy aukcyjnej lub kuriera, by telefonicznie skłonić do wygenerowania kodu B i jego przekazania.

Skala zjawiska jest poważna i ciągle rośnie. Policja odnotowuje setki takich przypadków, zarówno ujawnionych, jak i pozostających poza statystykami, co określa jako zjawisko o zatrważającej skali. Przykładowo, w samym tylko jednym śledztwie prowadzonym na Śląsku wykryto 127 oszustw metodą na B dokonanych w całej Polsce, w wyniku których poszkodowani stracili łącznie ponad 300 tysięcy złotych.

Ofiarami bywają osoby w różnym wieku, zarówno młodzi, obeznani z technologią użytkownicy portali społecznościowych, jak i starsi sprzedający przedmioty w internecie. Przestępcy stale modyfikują swoje metody i sięgają po nowe technologie, aby zwiększyć skuteczność ataków. Coraz częściej mówi się o wykorzystaniu audio-deepfake, czyli syntetycznego naśladowania głosu bliskiej osoby, by uwiarygodnić prośbę o pieniądze przesłaną w wiadomości głosowej. Ofiara może otrzymać nagranie brzmiące jak głos przyjaciela lub krewnego, błagającego o podanie kodu B – co czyni oszustwo jeszcze trudniejszym do rozpoznania i budzi w ofierze silne emocje, wyłączając zdrowy rozsądek. Eksperci ostrzegają, że dzięki takim technikom oszustwa na B wchodzą na wyższy poziom zagrożenia.

Oszustwa metodą na B rodzą szereg pytań prawnych dotyczących kwalifikacji takich zdarzeń oraz odpowiedzialności za powstałe szkody. Po stronie karnej, czyn polegający na wyłudzeniu kodu B i doprowadzeniu innej osoby do niekorzystnego rozporządzenia mieniem stanowi klasyczne oszustwo w rozumieniu art. 286 § 1 Kodeksu karnego. Sprawcy takich oszustw, jeśli zostaną ujęci, odpowiadają karnie – a gdy suma wyłudzeń jest znaczna lub proceder ma charakter stałego źródła dochodu, grożą im surowe kary (nawet do 15 lat pozbawienia wolności).

Wprowadzona w 2023 r. Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej dodatkowo typizuje przestępstwo podszywania się pod inną osobę w celu takiego wyłudzenia (tzw. smishing lub spoofing), co ma ułatwić ściganie sprawców posługujących się fałszywą tożsamością w rozmowach telefonicznych czy SMS.

Od strony prawa karnego ofiary mogą więc dochodzić sprawiedliwości poprzez zawiadomienie organów ścigania – choć, jak pokazuje praktyka, wykrywalność i



W.S.

ukaranie sprawców bywa utrudnione (zwłaszcza gdy działają oni z zagranicy lub wykorzystują tzw. słupy). Znacznie bardziej skomplikowana jest ocena prawna sytuacji ofiary w kontekście prawa cywilnego i bankowego, zwłaszcza jeśli chodzi o odzyskanie utraconych środków. Kluczową regulacją jest tu ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (implementująca unijną dyrektywę PSD), która normuje zasady odpowiedzialności za transakcje płatnicze wykonane bez zgody posiadacza rachunku. Zgodnie z tą ustawą co do zasady bank (dostawca usług płatniczych) ponosi odpowiedzialność za nieautoryzowane transakcje i powinien zwrócić klientowi skradzione pieniądze nie później niż do końca następnego dnia roboczego po zgłoszeniu reklamacji.

Bank może następnie dochodzić od posiadacza rachunku zwrotu kwoty, jeśli wykaże, że klient przyczynił się do transakcji umyślnie lub wskutek rażącego niedbalstwa.

Problem w tym, że w przypadku oszustwa na B formalnie rzecz biorąc transakcja jest autoryzowana przez samą ofiarę. Oszukany użytkownik sam wygenerował kod i zatwierdził operację w aplikacji bankowej, co z technicznego punktu widzenia oznacza, że wyraził zgodę na wypłatę środków.

Innymi słowy – nie doszło do nieuprawnionego użycia instrumentu płatniczego wbrew woli właściciela (jak ma to miejsce np. przy kradzieży karty czy włamaniu na konto bankowe bez wiedzy ofiary). Ofiara padła co prawda ofiarą podstępu, ale transakcja została wykonana z jej udziałem, po dokonaniu wymaganych autoryzacji (podania kodu i potwierdzenia PIN-em w aplikacji). Ta specyficzna sytuacja tworzy lukę w ochronie prawnej użytkowników mobilnych systemów płatności. Banki, powołując się na przepisy ustawy o usługach płatniczych oraz własne regulaminy, odmawiają uznania reklamacji klientów poszkodowanych metodą „na B " właśnie z argumentem, że transakcja nie była nieautoryzowana.

W ocenie banków wszelkie operacje potwierdzone prawidłowo przez użytkownika leżą po jego stronie ryzyka. Ofiary oszustw często dowiadują się, że nie doszło do naruszenia zabezpieczeń bankowych ani prawa bankowego, a jedynie do świadomego (choć wymuszonego podstępem) zlecenia płatności, za które bank nie bierze odpowiedzialności.

W świetle obowiązujących przepisów klienci mogą próbować dochodzić roszczeń na drodze cywilnej, powołując się np. na błędne wykonanie dyspozycji czy wprowadzenie w błąd co do tożsamości beneficjenta płatności, jednak szanse powodzenia takich działań są niewielkie. W praktyce Rzecznik Finansowy oraz UOKiK radzą poszkodowanym składać reklamacje i zawiadomienia na policję, choćby po to, by bank rzetelnie przeanalizował przypadek i zgłosił nadużycie



W.S.

organom ścigania. Jednak brak jednoznacznych regulacji nakazujących uznawanie roszczeń w sytuacji, gdy klient padł ofiarą socjotechniki, powoduje, że ofiary pozostają często bez ochrony finansowej.

Konsekwencje dla poszkodowanych.

Skutki oszustwa na B dla poszkodowanych są dotkliwe, zarówno pod względem finansowym, jak i emocjonalnym oraz prawnym. Przede wszystkim ofiara traci nieraz znaczne sumy pieniędzy – od kilkuset złotych po oszczędności życia, jeśli dała się nakłonić do wygenerowania wielu kodów lub wysokich kwot. Media regularnie opisują przypadki osób, które myśląc, że pomagają bliskim, straciły po kilka tysięcy złotych, a nawet wyższe kwoty.

Co gorsza, odzyskanie tych środków jest niezwykle trudne, a czasem niemożliwe.

Transakcje B mają charakter zbliżony do operacji gotówkowych – pieniądze wypłacone z bankomatu trafiają od razu w ręce oszusta i nie ma procedury chargeback (obciążenia zwrotnego), która chroniłaby płatności kartowe czy przelewy w przypadku oszustwa. Jeżeli ofiara zorientuje się w podstępie nawet kilka sekund po zatwierdzeniu transakcji, jest już za późno – bank ani operator systemu B nie są w stanie zatrzymać lub cofnąć transakcji, choć czy jest to pewne czy jedynie dla systemu finansowego wygodne, by brutalizują zaryzykować, tezę, że tanie.

W efekcie poszkodowany pozostaje z ubytkiem na koncie, który musi pokryć z własnych środków. Wielu oszukanych klientów banków przeżywa dodatkowo ogromną frustrację w zetknięciu z procedurą reklamacyjną. Banki z reguły odrzucają reklamacje w takich sytuacjach, argumentując, że klient sam potwierdził operację i tym samym ponosi pełną odpowiedzialność. Z punktu widzenia prawa cywilnego ofiara staje się więc osobą, która sama – choć pod wpływem błędu – rozporządziła swoimi pieniędzmi, co ogranicza możliwości dochodzenia zwrotu. Poszkodowany może mieć poczucie bezsilności i braku wsparcia instytucjonalnego. Co prawda, istnieje możliwość zwrócenia się o pomoc do Rzecznika Finansowego lub rzeczników konsumentów, a także dochodzenia roszczeń na drodze sądowej, ale procesy te są długotrwałe i niepewne. W międzyczasie ofiara ponosi pełnię szkody finansowej, co bywa szczególnie dotkliwe dla osób gorzej sytuowanych. Oprócz strat majątkowych pojawiają się też konsekwencje prawne pośrednie. Jeśli oszustwo „na B ” było elementem szerszego działania przestępczego (np. połączonego z wyłudzeniem danych osobowych ofiary), poszkodowany może paść ofiarą dalszych nadużyć – na jego dane mogą zostać zaciągnięte pożyczki lub zawarte umowy kredytowe. Z tego względu niezmiernie ważne jest, aby osoba, która padła ofiarą

takiego oszustwa, niezwłocznie powiadomiła swój bank i policję oraz zabezpieczyła swoje dane (np. zastrzegła dokumenty tożsamości, zmieniła hasła itp.)

Zgłoszenie incydentu pozwala też udokumentować nasz brak winy w ewentualnych kolejnych zdarzeniach (np. gdyby przestępcy dalej wykorzystywali wyłudzone informacje). Ponadto ofiary doznają często uszczerbku emocjonalnego. Obok szoku i stresu związanego z nagłą utratą pieniędzy, pojawia się poczucie upokorzenia, żalu do siebie (za naiwną ufność) oraz utrata zaufania do kontaktów internetowych. Często ofiara dopiero po fakcie uświadamia sobie, jak misternie została zmanipulowana. Dla niektórych wiąże się to z długotrwałym poczuciem niepewności, obawą przed korzystaniem z bankowości elektronicznej czy mediów społecznościowych.

Oszustwa na B . obnażają istotny problem asymetrii ryzyka pomiędzy użytkownikami a instytucjami finansowymi. W obecnym modelu to klient ponosi niemal całe ryzyko związane ze współczesnym cyfrowym zaborem, podczas gdy banki i operatorzy płatności mobilnych chronią się zapisami o autoryzacji transakcji.

System B sam w sobie spełnia wymagane standardy bezpieczeństwa technicznego – każda transakcja wymaga podania jednorazowego kodu i jej potwierdzenia w aplikacji za pomocą PIN lub biometrii. Jednak ta dwuetapowa autoryzacja jest skuteczna jedynie przeciw nieuprawnionemu dostępowi technicznemu, nie zabezpiecza zaś przed socjotechniką. Przestępcy z premedytacją wykorzystują czynnik ludzki jako najsłabsze ogniwo systemu – omijają zabezpieczenia nie poprzez ich złamanie, ale nakłaniając ofiarę do współpracy. Z punktu widzenia banku transakcja przebiegła poprawnie, dlatego instytucja finansowa „umywa ręce" od odpowiedzialności, pozostawiając klienta z problemem.

Postawa banków jest coraz częściej krytykowana jako niewystarczająca wobec skali zjawiska i profesjonalizmu oszustów. Banki bronią się, że nie mogą odpowiadać za błędy użytkowników, zwłaszcza że w regulaminach usług wyraźnie zakazują udostępniania komukolwiek kodów czy haseł. W praktyce jednak przeciętny konsument narażony jest na atak wyrafinowanymi metodami manipulacji, na które nie jest przygotowany. Brak proaktywnej reakcji ze strony instytucji finansowych powoduje, że oszustwo na B stało się dla cyberprzestępców najbezpieczniejszym narzędziem do wyłudzania pieniędzy – gdyż umożliwia szybkie uzyskanie gotówki, a jednocześnie minimalizuje ryzyko finansowe po stronie banku.

Policja wprost ostrzega, że dla płatności między osobami prywatnymi B jest obecnie preferowanym przez oszustów kanałem i radzi unikać go „jak ognia" przy transakcjach z nieznajomymi.

W.G.

W przeciwieństwie do kart płatniczych czy przelewów, gdzie istnieją procedury blokady środków i chargebacku, w systemie B . brak jest wbudowanych mechanizmów ochronnych dla ofiar nadużyć. To sprawia, że ciężar finansowy konsekwencji spoczywa na kliencie, podczas gdy bank nie ponosi straty – taka dysproporcja zachęca oszustów do dalszego działania, bo wiedzą oni, że bank nie będzie ich aktywnie ścigał na rzecz klienta (co innego w przypadku klasycznych nieautoryzowanych włamań, gdzie bank musi zwrócić środki i ma interes w odzyskaniu pieniędzy).Warto zauważyć, że system B . i banki mogłyby teoretycznie wprowadzić dodatkowe zabezpieczenia ograniczające skuteczność „metody na znajomego". Przykładowo, aplikacje bankowe mogłyby bardziej wyeksponować informację o miejscu i sposobie realizacji transakcji przy prośbie o potwierdzenie (obecnie nazwa miasta lub punktu wypłaty bywa widoczna w powiadomieniu push, ale ofiary często ją ignorują.

Gdyby system wykrywał anomalię – na przykład nietypową porę, dużą kwotę czy geograficzne oddalenie między urządzeniem użytkownika a bankomatem – mógłby zastosować dodatkową weryfikację lub ostrzeżenie. Niestety, takie inteligentne mechanizmy nie są powszechnie wdrożone, a edukacyjne komunikaty ostrzegawcze często pojawiają się dopiero po fakcie (np. kampanie informacyjne policji czy komunikaty w mediach). Banki jak dotąd skupiają się głównie na ochronie przed technicznym złamaniem zabezpieczeń, natomiast ochrona przed oszustwem socjotechnicznym pozostaje niedopracowana, co stanowi słaby punkt całego systemu.

W obliczu narastającej fali oszustw metodą na B . potrzebne są wielotorowe działania zaradcze – zarówno legislacyjne i regulacyjne, jak i technologiczne oraz edukacyjne. Poniżej przedstawiono kluczowe rekomendacje, które mogłyby poprawić ochronę konsumentów i bardziej zrównoważyć odpowiedzialność między klientami a instytucjami finansowymi.

Zmiany legislacyjne w zakresie odpowiedzialności za transakcje oszukańcze.

Należałoby rozważyć nowelizację ustawy o usługach płatniczych lub wprowadzenie odrębnych przepisów, które wprost adresowałyby sytuację transakcji dokonanych pod wpływem podstępu (social engineering). Celem byłoby uznanie, że transakcja wyłudzona od konsumenta podstępnie jest równoważna transakcji nieautoryzowanej, co obligowałoby bank do zwrotu pieniędzy ofierze w krótkim terminie. Obecne przepisy nie precyzują tego wprost, więc doprecyzowanie definicji „nieautoryzowanej transakcji" o przypadki, gdy wprawdzie doszło do autoryzacji, ale bez świadomej intencji przelania środków na rzecz oszusta, zamknęłoby lukę wykorzystywaną przez banki do uchylania się od odpowiedzialności. Takie

rozwiązania są dyskutowane w innych jurysdykcjach – np. w niektórych krajach wdraża się mechanizmy obowiązkowego rekompensowania strat ofiarom oszustw „authorized push payment" (przelewów autoryzowanych przez ofiarę pod wpływem oszustwa). W Polsce mógłby powstać fundusz kompensacyjny z udziałem banków, z którego pokrywane byłyby tego rodzaju szkody, co skłoniłoby banki do większej dbałości o prewencję.

Wzmocnienie regulacji nadzorczych. Komisja Nadzoru Finansowego oraz Narodowy Bank Polski mogłyby wydać wytyczne lub rekomendacje dla banków, zobowiązujące je do aktywniejszej ochrony klientów przed tego typu oszustwami. Mogłyby one obejmować m.in. obowiązek wdrażania systemów wykrywania podejrzanych transakcji B (np. sekwencyjne wielokrotne wypłaty maksymalnych kwot w krótkim czasie, co jest charakterystyczne dla działania oszustów), czy nałożenie na banki wymogu czasowego wstrzymania realizacji transakcji budzącej wątpliwości i potwierdzenia jej innym kanałem.

Również procedury reklamacyjne powinny ulec zmianie. Obecnie banki często z góry odrzucają reklamacje ofiar oszustwa na B , tymczasem nadzór finansowy mógłby wymagać, by każdy przypadek był indywidualnie analizowany z uwzględnieniem okoliczności (np. czy klient mógł racjonalnie rozpoznać podstęp). Brak należytej staranności banku w ostrzeżeniu klienta czy udaremnieniu oczywiście podejrzanej transakcji mógłby skutkować nałożeniem nań częściowej odpowiedzialności.

Zwiększenie odpowiedzialności i zaangażowania operatora systemu B . (operator B ) oraz banki-partnerzy systemu powinny wspólnie opracować dodatkowe zabezpieczenia transakcji oraz procedury awaryjne. Można rozważyć opcję wprowadzenia dodatkowego uwierzytelnienia przy wypłatach B na większe kwoty lub w przypadku transakcji zainicjowanych w niestandardowy sposób (np. gdy kod jest wykorzystany do wypłaty w odległej lokalizacji względem urządzenia ofiary). Innym pomysłem jest wdrożenie mechanizmu opóźnionego zatwierdzenia – tzn. danie użytkownikowi np. 15–30 sekund na ewentualne anulowanie transakcji już po jej zatwierdzeniu, co mogłoby pomóc, gdy ofiara zorientuje się niemal od razu (obecnie nawet kilkusekundowe opóźnienie nic nie daje). Operator systemu mógłby także stworzyć dedykowany tryb reklamacyjny dla B , w którym sporne transakcje są od razu monitorowane pod kątem próby wypłaty gotówki – w porozumieniu z policją możliwe byłoby np. szybkie namierzenie oszusta przy bankomacie (co już czasem się udaje przy zgłoszeniu natychmiastowym, ale nie jest to sformalizowane).

W.S.

Edukacja i prewencja. Równie ważnym elementem jest zwiększanie świadomości użytkowników. Banki i instytucje publiczne powinny prowadzić intensywne kampanie informacyjne ostrzegające przed metodą „na B ". Krótkie komunikaty mogłyby być wbudowane w same aplikacje bankowe – np. przy generowaniu kodu B pojawiałoby się wyraźne ostrzeżenie: „Uważaj – czy na pewno znasz osobę, która prosi o ten kod? To może być oszustwo!". Warto uczyć społeczeństwo, by zawsze weryfikować tożsamość osoby proszącej o pomoc finansową (choćby przez wykonanie telefonu weryfikującego zamiast polegania na samym komunikatorze), a także by czytać uważnie komunikaty przy zatwierdzaniu transakcji (szczególnie informacje o miejscu wypłaty). Podnoszenie świadomości cyfrowej użytkowników – np. szkolenia z rozpoznawania manipulacji, informacji o nowych technikach typu deepfake – może znacząco utrudnić zadanie oszustom. Instytucje państwowe (UOKiK, policja) już prowadzą takie działania, ale powinny one objąć szersze kręgi, w tym osoby młode, które – paradoksalnie – bywają bardziej ufne wobec kontaktów online i padają ofiarą tej metody.

Współpraca sektorowa. Problem oszustw finansowych jest złożony, dlatego wymaga współpracy między bankami, organami ścigania a operatorami telekomunikacyjnymi. Należy usprawnić mechanizmy wymiany informacji o zagrożeniach – np. banki mogłyby szybko dzielić się danymi o nowych schematach oszustw z innymi bankami i policją. Również operatorzy portali społecznościowych powinni włączyć się w ten wysiłek: szybkie reagowanie na zgłoszenia przejęcia konta, udaremnianie masowego rozsyłania wiadomości przez boty, a także ułatwienia dla użytkowników w zgłaszaniu podejrzanych aktywności (tak, by np. znajomi mogli ostrzec, że konto zostało przejęte, zanim dojdzie do wyłudzeń). Dzięki takiej współpracy można by ograniczyć czas działania oszusta i zminimalizować liczbę ofiar w danej kampanii przestępczej.

Oszustwa metodą na B stały się poważnym wyzwaniem dla bezpieczeństwa finansowego konsumentów w dobie płatności mobilnych. Wykorzystując technologię i psychologię – od przejmowania kont na portalach społecznościowych, przez masowe wysyłanie wiadomości i połączenia, aż po deepfake – przestępcy omijają tradycyjne zabezpieczenia systemów bankowych i wyłudzają miliony złotych rocznie kosztem niczego niepodejrzewających ofiar. Analiza problemu ujawnia, że obecny stan prawny i praktyka banków nie zapewniają wystarczającej ochrony pokrzywdzonym. Ofiary często pozostają same z finansowymi skutkami oszustwa, podczas gdy sprawcy wykorzystują asymetrię odpowiedzialności na swoją korzyść. Aby przywrócić równowagę i zaufanie do systemu płatności, konieczne są zdecydowane działania. Postulaty na przyszłość obejmują m.in. uzupełnienie luk prawnych tak, by ofiary oszustw socjotechnicznych nie były pozostawione bez



W.G.

ochrony prawnej, a banki ponosiły proporcjonalną część ryzyka takich operacji. Równocześnie banki i operatorzy płatności powinni zainwestować w udoskonalenie zabezpieczeń oraz procedur monitorowania transakcji, wykraczając poza minimalne wymogi i uwzględniając czynnik ludzki w modelach ryzyka. Nie mniej ważna jest profilaktyka – edukowanie użytkowników i budowanie w nich nawyków ostrożności w kontaktach online. Tylko kompleksowe podejście, łączące regulacje prawne, odpowiedzialność instytucjonalną i świadomość społeczną, pozwoli ograniczyć żniwo, jakie zbierają oszustwa na B .

W przyszłości należy dążyć do systemu, w którym szybkość i wygoda płatności będą szły w parze z bezpieczeństwem, a zaufanie klientów do bankowości elektronicznej nie będzie nadszarpywane przez tego typu przestępstwa. Wnioskiem płynącym z powyższej analizy jest jasno dostrzeżona potrzeba wzmocnienia ochrony prawnej konsumentów i zwiększenia aktywnej roli banków w zapobieganiu oraz rekompensowaniu skutków oszustw – tak, aby nie powtarzały się historie klientów pozostawionych samym sobie po tym, gdy padli ofiarą perfidnej manipulacji.

Glosa do problematyki nieautoryzowanych transakcji płatniczych, w szczególności w obszarze tzw. kradzieży „na B ", wymaga wnikliwego spojrzenia na relację pomiędzy obowiązkami i odpowiedzialnością dostawcy usług płatniczych a pozycją, jaką zajmuje klient, będący z reguły stroną słabszą w sporze z instytucją finansową.

Zgodnie z art. 45 ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, ciążący na banku obowiązek wykazania faktu autoryzowania transakcji stanowi wyraz zasady przerzucenia ryzyka technologicznego i organizacyjnego na instytucję profesjonalną. Ratio legis tego przepisu zdaje się dobitnie ilustrować koncepcję, wedle której to właśnie wyspecjalizowana jednostka finansowa, dysponująca zasobami i wiedzą ekspercką, jest najlepiej predestynowana do monitorowania i zapobiegania oszustwom płatniczym. Cogito ergo sum – parafraza kartezjańskiej maksymy mogłaby tutaj wybrzmieć w formie postulatu „sophus ergo responde" – mądry (profesjonalista) niechaj ponosi brzemię odpowiedzialności za niedostatki systemu, który został przez niego wprowadzony i wykorzystywany.

Istotę sporu w przypadku oszustw „na B " stanowi brak lub iluzoryczność autentycznej woli klienta, który przekazuje kod i potwierdza transakcję w przeświadczeniu, że pomaga osobie bliskiej, zaś w rzeczywistości działa w warunkach błędu wywołanego przez manipulację sprawcy. Social engineering, rozumiany jako zespół technik psychologicznych zmierzających do wyłudzenia autoryzacji, jest zjawiskiem powszechnym i dobrze rozpoznanym w literaturze przedmiotu. Ten sposób działania oszustów, żerujących na ludzkiej empatii, konstruuje na gruncie

prawa płatniczego stan faktyczny, w którym zgoda (consensus) nie występuje, a jeśli już – to w okolicznościach, które każą taką rzekomą zgodę uznać za dotkniętą wadą oświadczenia woli w rozumieniu przepisów Kodeksu cywilnego (błąd, podstęp). W tym świetle bank, chcąc uchylić się od odpowiedzialności, powinien wykazać, iż zachowanie klienta wyczerpywało znamiona rażącego niedbalstwa, albowiem bez tego nie może skutecznie przerzucić nań ciężaru finansowego nieautoryzowanej płatności.

Oceniając kategorię rażącego niedbalstwa w rozumieniu art. 46 ust. 3 i n. ustawy o usługach płatniczych, należy przywołać utrwaloną w judykaturze wykładnię, zgodnie z którą rażące niedbalstwo oznacza zachowanie odbiegające w stopniu kwalifikowanym od elementarnej staranności, jakiej wymaga się w stosunkach społecznych od przeciętnej osoby. Podkreślają to liczne orzeczenia Sądu Najwyższego, w tym wyrok z dnia 22 kwietnia 2004 r., sygn. II CK 142/03, w którym Sąd Najwyższy wskazał, że bank – będąc instytucją zaufania publicznego – nie może przenosić całego ryzyka gospodarczego związanego z funkcjonowaniem systemu płatniczego na klienta. Podobnie wypowiedział się Sąd Najwyższy w wyroku z dnia 18 stycznia 2018 r., sygn. V CSK 141/17, stwierdzając, iż bank winien w sposób niebudzący wątpliwości wykazać, że to sam użytkownik „autoryzował" sporną transakcję, a więc że świadomie i w pełni dobrowolnie zainicjował proces przelania środków na rzecz określonego odbiorcy. Autoryzacja to wszak nie tylko mechaniczne wpisanie kodu czy kliknięcie w aplikacji, lecz świadomy akt woli. Gdy ową wolę wykrzywił błąd wywołany oszustwem, brak jest podstaw do przyjęcia, iż doszło do właściwej autoryzacji.

W kontekście silnego uwierzytelniania klienta (Strong Customer Authentication – SCA), wymaganego przepisami Dyrektywy (UE) 2015/2366 (PSD2) oraz uściślonego Wytycznymi Europejskiego Urzędu Nadzoru Bankowego (EBA) z 21 czerwca 2019 r. nr EBA-Op-2019-06, należy zauważyć, że krajowe instytucje finansowe często poprzestają na uproszczonych procedurach weryfikacyjnych. System B bywa przedstawiany jako udogodnienie, a niekiedy słusznie krytykowany jest za brak pełnej dwu- lub trójelementowej autentykacji, która sprzyjałaby minimalizacji ryzyka nieautoryzowanych transakcji. Nie sposób pominąć tu starorzymskiej paremii vigilantibus iura scripta sunt – prawa tworzone są dla osób zachowujących czujność – która jednak w dobie nowoczesnych technologii staje się niewystarczająca, gdyż brak równowagi informacyjnej pomiędzy bankiem a klientem podważa skuteczność działania tej zasady. Klient dokonuje czynności w przekonaniu, iż bank zapewnił właściwe zabezpieczenia, podczas gdy bank może dążyć do przerzucenia winy na „nieuważnego" użytkownika.

Takie rozumowanie prowadzi nas na grunt kantowskiej filozofii moralnej, w szczególności do imperatywu kategorycznego, który nakazuje traktować drugiego człowieka zawsze jako cel, a nigdy wyłącznie jako środek. Nie powinno się zatem godzić, by zysk banku, generowany przez skracanie czy upraszczanie procedur, przekładał się na systemowe lekceważenie bezpieczeństwa konsumentów, traktowanych wyłącznie jako źródło prowizji lub opłat. Zgodnie z duchem myśli Immanuela Kanta postępowanie instytucji finansowych powinno opierać się na zasadach, które można by uczynić powszechnymi prawami moralnymi i prawnymi, a jedną z nich bezsprzecznie jest konieczność zapewnienia realnej ochrony klienta przed oszustwem, w oparciu o przejrzyste i solidne mechanizmy weryfikacyjne.

W praktyce, próbując uchylić się od roszczeń klienta, bank powołuje się często na twierdzenie, że klient rzekomo „osobiście" autoryzował transakcję, wprowadzając kod B czy potwierdzając płatność w aplikacji. Stoi to jednak w sprzeczności z literalnym brzmieniem art. 45 ust. 1 ustawy o usługach płatniczych, z którego jasno wynika, że to nie klient ma udowodnić, iż nie autoryzował płatności, lecz bank musi wykazać, że zgoda klienta została wyrażona w sposób świadomy i wolny od wad oświadczenia woli. Nie sposób też zapomnieć, iż w kontekście orzecznictwa, w tym przywołanego wyroku Sądu Najwyższego z dnia 18 stycznia 2018 r., V CSK 141/17, zgoda wyrażona pod wpływem podstępu lub w błędzie co do tożsamości osoby, na rzecz której przekazywane są środki, nie jest zgodą w sensie obowiązujących przepisów.

Podkreślić należy, że kwestia rażącego niedbalstwa w takich sytuacjach bywa nadmiernie eksponowana przez banki, które pragną uchylić się od obowiązku niezwłocznego zwrotu środków. Nie każde zaufanie do bliskiego czy znajomego (nawet komunikującego się za pośrednictwem M ) można kategoryzować jako rażące niedbalstwo. Zgodnie z dominującą linią orzeczniczą w tym zakresie (m.in. wyrok SN z 22 kwietnia 2004 r., II CK 142/03) rażące niedbalstwo to wada postępowania o charakterze kwalifikowanym, kiedy dochodzi do braku elementarnej przezorności. Zwykły ludzki odruch, zgodny z przejawem naturalnej empatii oraz socjalizacyjnych schematów, nie musi być oceniany jako ewidentne i skrajnie lekkomyślne zlekceważenie ostrzeżeń, które system bankowy powinien zapewniać. Dodatkowo, przy zaniechaniu przez bank stosownych mechanizmów monitorowania transakcji (chociażby wstrzymania wypływu środków w sytuacjach podejrzanych lub nietypowych), trudno winić klienta za to, że – czasem w krótkiej chwili nieuwagi – padł ofiarą manipulacji.

W świetle powyższego należy postulować, by banki wprowadziły skuteczniejsze środki ochrony, co jest ich obowiązkiem wynikającym z zarówno dyrektywy PSD2,

jak i z podstawowej zasady ochrony konsumenta. Argument, iż dodatkowe procedury wydłużają czas transakcji, nie powinien przeważać nad koniecznością zapewnienia bezpieczeństwa. Stanowisko takie jest zresztą konsekwencją od dawna wyznawanej w doktrynie zasady favor debitoris w prawie zobowiązań oraz zasady in dubio contra proferentem przy interpretacji wzorców umownych, co dodatkowo wspiera klienta w sporze z instytucją finansową.

Podsumowując, w sporach dotyczących nieautoryzowanych transakcji z użyciem B , na banku spoczywa ciężar dowodu udowodnienia, iż klient w sposób świadomy zaakceptował daną płatność. Autoryzacja nie sprowadza się do banalnego stwierdzenia, że „klient miał w ręku telefon i wpisał kod", lecz wymaga wykazania autentycznej i nieobciążonej wadami woli dokonania przekazu środków określonemu odbiorcy. Jeżeli taka wola nie istnieje bądź została wykrzywiona przez błąd wprowadzony podstępem, mamy do czynienia z nieautoryzowaną transakcją w rozumieniu ustawy o usługach płatniczych. W świetle spójnej linii orzeczniczej Sądu Najwyższego, a także zgodnie z nakazami kantowskiej etyki, bank nie powinien uchylać się od rekompensaty, powołując się na argumenty podające w wątpliwość zwykłe, ludzkie zachowania klienta. Człowiek, kierujący się naturalnym odruchem pomocy osobie, którą subiektywnie uznaje za przyjaciela, nie postępuje w sposób karygodnie lekkomyślny, a bank, jeśli przyjmuje na siebie rolę profesjonalnego dostawcy usług płatniczych, winien brać na siebie ryzyko technologiczno-organizacyjne i ponosić konsekwencje niedostatków w zakresie stosowania silnego uwierzytelniania oraz systemów bezpieczeństwa. *Salus rei publicae suprema lex esto* – bezpieczeństwo obrotu finansowego powinno stanowić nadrzędne dobro, którego ochrona spoczywa w pierwszej kolejności na profesjonalnych uczestnikach rynku, aby klient nie był pozostawiony sam na pastwę oszukańczych praktyk i społecznych inżynierii.

Minął ponad rok od przejęcia władzy, okres prób, analiz i raportów dobiegł końca. Nadszedł moment na konkretne decyzje legislacyjne, zwłaszcza że wkrótce głos rozstrzygający nie będzie należał do Prezydenta Andrzeja Dudy, a argumenty o rzekomej blokadzie podpisu ustawy tracą moc.

Ustawa o petycjach z całą mocą zobowiązuje organy władzy do szybkiego i merytorycznego rozpatrywania głosu społecznego, tymczasem upowszechnia się praktyka pozorowania. Petycje giną w czeluściach urzędów, a terminy, jakże hojnie określone w ustawie na zaledwie trzy miesiące, rozciągają się w nieskończoność. Zważcie proszę o obowiązku niezwłoczności publikacji treści petycji, zwyczajowo przyjmowanej na dwa tygodnie od złożenia. Władza ma szanować prawo i suwerena.

Nie jest rolą obywatela tworzyć analizy i projekty ustaw, od tego są rządzący, którzy pobierają środki z pieniędzy publicznych. Gdy więc obywatele sygnalizują problem, oczekują decyzji bądź jasnego, otwartego głosowania, w którym władza weźmie odpowiedzialność za utrzymanie status quo lub za przeprowadzenie zmian.

Dosyć złudzeń o rzekomej niemożności. Reforma państwa i konstrukcji prawa to obowiązek tych, którzy rządzą, i nie uchyla się od niego nikt, kto naprawdę dba o dobro Polski. Przywoływanie argumentu o presji partyjnych liderów i zakulisowych decyzjach jedynie uwłacza godności tych, którzy objęli mandaty z woli narodu.

Zatem porzućmy pozoranctwo. Zapowiedzi i obietnice wyborcze powinny wreszcie przełożyć się na realne decyzje. Macie pełnię instrumentów i uprawnień, więc rządźcie odpowiedzialnie albo powiedzcie jasno, że wolicie pozostawić sprawy po staremu. Jednak nie zapominajcie, że to Wy składaliście narodowi uroczyste deklaracje, a naród, kierując się rozsądkiem i wolą wspólnego dobra, może w następnych wyborach zweryfikować, czy umiecie sprostać powierzonej Wam misji.

Uprzejmie informujemy, że Katarzyna Kosakowska oraz Witold Solski w imieniu Kancelarii Doradczej Solski i Partnerzy sp. z o.o. wykonują zawodową działalność lobbingową. Działamy w przestrzeni ochrony praw człowieka, troszczymy się o wolność i własność, bronimy godności ludzkiej.

Niniejszą petycję składamy na rzecz Fundacji Dobre Państwo, reprezentując Fundację jako podmiot wykonujący zawodową działalność lobbingową w procesie stanowienia prawa.

Wskazujemy przy tym, że petycje są – dzięki powszechnej dostępności - jedyną realną gwarancją bezpośredniego udziału społeczeństwa w procesie ustawodawczym. Ich umiejscowienie w systemie prawnym w sposób jednoznaczny odróżnia je od skarg czy wniosków, co wskazuje, że petycje to instrument służący przede wszystkim ochronie dobra wspólnego i życia zbiorowego. Tak też powinny być traktowane przez organy je rozpatrujące.

Prezydent RP i każda komisja parlamentarna mają niezwykle ważną z tej perspektywy prerogatywę – inicjatywę legislacyjną. Załatwienie przez organ władzy sprawy w rozumieniu ustawy o petycjach może więc polegać na podjęciu działań prawotwórczych. O te właśnie postulujemy, wskazując, że zmiana prawa, której się domagamy, jest istotna zwłaszcza w kontekście dobra wspólnego.

Ustawa o petycjach, ustawa o lobbingu oraz inne przepisy regulują zasady udziału organizacji społecznych, również tych reprezentowanych przez lobbystów, w procesie stanowienia prawa. Odwołując się do tych przepisów prosimy o

wskazanie terminu posiedzenia Komisji, na którym nasza petycja będzie rozpatrywana oraz o informację o sposobie załatwienia naszej sprawy.

## OŚWIADCZENIE

Wyrażamy zgodę na publikację petycji z podaniem nazwy oraz wszystkich danych kontaktowych i identyfikacyjnych podmiotu składającego Petycję oraz naszych imion i nazwisk jako osób podmiot ten reprezentujących.

z wyrazami szacunku,

**Witold Solski** | **Katarzyna Kosakowska**