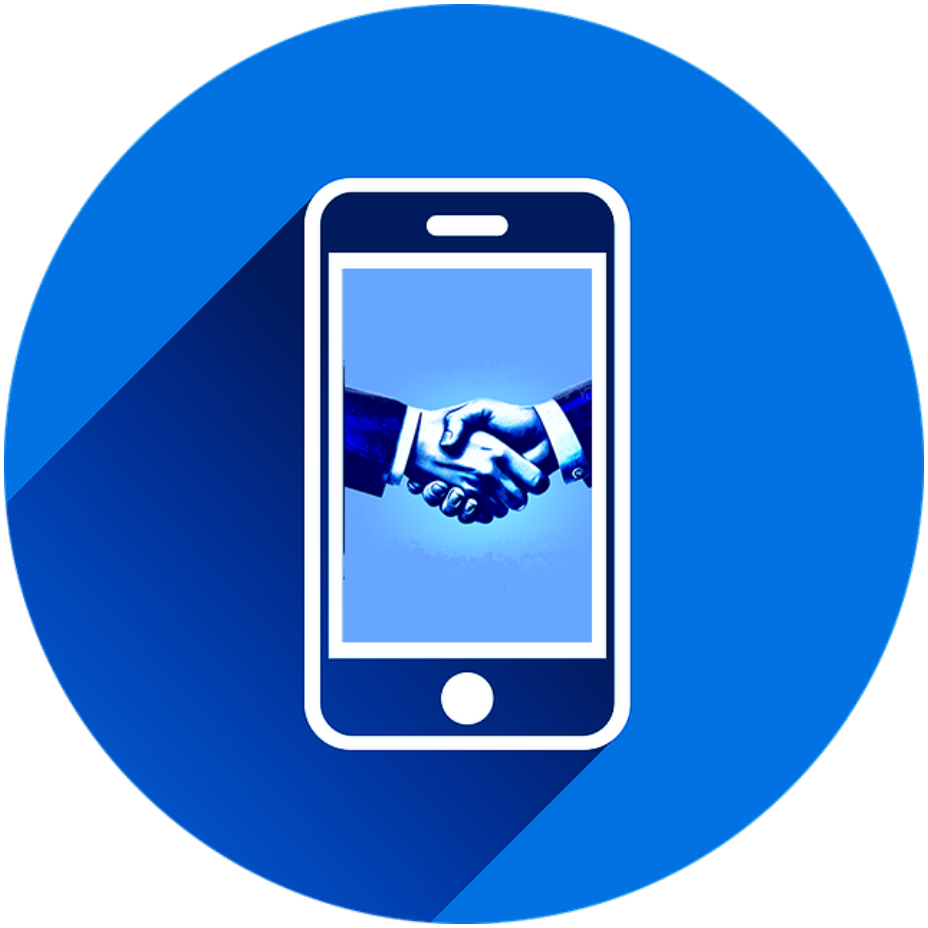
Rzecznik Finansowy

www.rf.gov.pl

PORADNIK RZECZNIKA FINANSOWEGO W SPRAWIE PROBLEMATYKI TZW. „KREDYTÓW NA KLIK" I NIEAUTORYZOWANYCH TRANSAKCJI PŁATNICZYCH

Lawinowo rośnie liczba wniosków do Rzecznika Finansowego o rozpatrzenie zastrzeżeń klientów dotyczących dochodzenia roszczeń przez banki z umów kredytów, jak twierdzą klienci – niezawieranych świadomie przez nich, tylko na skutek działań cyberprzestępców, z wykorzystaniem socjotechnik i metod hakerskich.

W niniejszym poradniku Rzecznik Finansowy przedstawia wyniki przeprowadzonej analizy problematyki, a także informacje mające na celu ochronę konsumentów przed tego rodzaju oszustwami.



Czym jest „Kredyt na klik"?

Wyłudzenie środków tzw. metodą „kredyt na klik" jest częścią szerszego działania przestępców specjalizujących się w przestępstwach finansowych. Ich działania wiążą się z wyłudzeniem danych, pozwalających na dostęp do kanałów komunikacji elektronicznej pomiędzy bankiem a klientem (np. dotyczących bankowości elektronicznej). W następstwie takiego niewychwyconego w porę i niezatrzymanego działania, wyprowadzane są środki z rachunków bieżących, likwidowane są lokaty czy inne produkty inwestycyjne, a następnie zaciągane zobowiązania w imieniu osoby poszkodowanej – w tym obciążanie kart kredytowych oraz wzięcie „kredytu na klik".

Poprzez tzw. „kredyty na klik" należy rozumieć zawarcie umowy o kredyt konsumencki (zgodnie ustawową z definicją kredytu konsumenckiego włącza się do niego również umowy pożyczki[1]), zawierane na odległość z wykorzystaniem najczęściej bankowości elektronicznej lub aplikacji mobilnej, w przypadku których do złożenia oświadczenia woli o chęci zawarcia takiej umowy wykorzystuje się z reguły indywidualne dane uwierzytelniające[2] po uprzedniej zautomatyzowanej weryfikacji zdolności kredytowej i wstępnie przygotowanej na tej podstawie ofercie kredytowej, bez kontaktu klienta z pracownikiem banku. Oferta takiej umowy jest dostępna „od ręki" dla niemal każdego zalogowanego w bankowości elektronicznej albo aplikacji mobilnej, gdyż przygotowywana jest ona automatycznie, zwykle z zastosowaniem algorytmów bankowych (w tym tzw. scoringowych – czyli w oparciu o historię uznań i obciążeń danego rachunku) i nie wymaga wizyty w oddziale albo podania dodatkowych informacji przez klienta. Wniosek składa się on-line i wymaga on, zgodnie z art. 7 ust. 1 ustawy Prawo bankowe, zatwierdzenia w postaci elektronicznej (do czego wykorzystuje się indywidualne dane uwierzytelniające analogiczne jak dla składania zleceń płatniczych). Nie są to jednak transakcje płatnicze w rozumieniu art. 2 pkt 29 ustawy o usługach płatniczych.

W przypadku wyłudzenia metodą „kredyt na klik" do zawarcia umowy kredytu dochodzi bez zgody i wiedzy klienta banku, a więc jego świadomości. W typowym scenariuszu dla tego rodzaju spraw klient, który pada ofiarą ataku socjotechnicznego (z wykorzystaniem przede wszystkim metody określanej jako *vishing*[3], a w jej ramach dodatkowo *spoofing*[4]), na skutek manipulacji i oszustw przekazuje przestępcom, np. dostęp do swojego urządzenia poprzez zdalny pulpit czy kody autoryzacyjne z wiadomości SMS, które następnie wykorzystywane są przez nich do składania nie tylko zleceń płatniczych, ale także „potwierdzania" chęci zawarcia umowy „kredytu na klik" na podstawie opisanych wyżej ofert przygotowanych dla klienta w bankowości elektronicznej albo aplikacji mobilnej. W ten sposób niczego nieświadoma osoba „potwierdza" zawarcie umowy i zostaje obciążona zobowiązaniem związanym

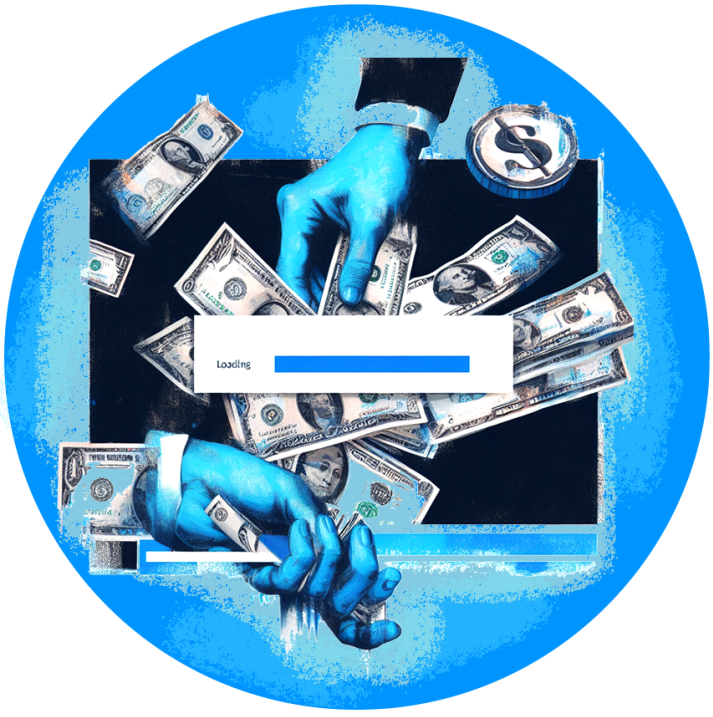
[1] Art. 3 ust 2 ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim (t.j. Dz. U. z 2023 r. poz. 1028 ze zm.).
[2] W rozumieniu art. 2 pkt 9d ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych – dalej ustawa o usługach płatniczych albo UUP
[3] Vishing to pozyskanie informacji poufnej przez przestępców z wykorzystaniem telefonu. Przestępca wyłudza dane podszywając się pod osoby lub instytucje godne zaufania.
[4] Spoofing to rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, firmy, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy. Dzięki wykorzystaniu różnych technik, oszuści mogą podszyć się pod wybrany adres e-mail, numer telefonu, a nawet adres IP i w nieuczciwy sposób osiągnąć swoje cele.

z zawarciem „kredytu na klik”, podczas gdy środki w ten sposób uzyskane z banku są transferowane przez przestępców na inne rachunki bankowe.

Analiza przeprowadzona przez Rzecznika Finansowego - narzucanie klientom otrzymywania ofert lub możliwości zawierania umów

Z badań przeprowadzonych przez Rzecznika Finansowego wynika, że w zdecydowanej większości banków w ramach zawierania umowy o świadczenie usługi prowadzenia rachunku płatniczego **klient nie ma możliwości niewyrażenia zgody (rezygnacji) na zawieranie umów w formie „kredytów na klik”**, tj. na podstawie przygotowywanych dla niego ofert w bankowości elektronicznej lub aplikacji mobilnej. To oznacza, że jeśli klient chce korzystać z rachunku płatniczego w banku, otrzymuje wzór umowy oraz jej integralnych części – regulaminów, w których adhezyjnie (automatycznie) zawarto postanowienia dot. możliwości zawierania umów kredytów on-line, z wykorzystaniem indywidualnych danych uwierzytelniających (zasadniczo służących do składania zleceń płatniczych w bankowości elektronicznej czy aplikacji mobilnej).

Część banków wskazuje w tym kontekście na możliwość niewyrażenia tzw. zgód marketingowych na przedstawianie ofert zawarcia kredytów na klik on-line, jednak nie jest to z punktu widzenia działań socjotechnicznych oszustów znacząca przeszkoda, gdyż zmiana zgody odbywa się poprzez kliknięcie tzw. *checkboxa* w bankowości elektronicznej lub aplikacji mobilnej, co nie stanowi przeszkody w przypadku wyłudzenia danych uwierzytelniających (dostępowych) klienta.



Jak się ochronić?

Z punktu widzenia klienta banku, środki ochrony przed tego rodzaju oszustwami są analogiczne jak w przypadku oszustw związanych z kradzieżą środków z rachunków płatniczych (czyli dokonywania nieautoryzowanych transakcji płatniczych).

Warto przypomnieć w tym kontekście, że Rzecznik Finansowy przyłączył się do ogólnopolskiej kampanii społecznej „Stracisz dane, stracisz pieniądze!" zainicjowanej przez Prezesa UOKiK (więcej informacji tutaj:

https://rf.gov.pl/2023/01/10/ogolnopolska-kampania-spoleczna-stracisz-dane-stracisz-pieniadze/).

Należy pamiętać, aby **bezwzględnie nie podawać żadnych danych uwierzytelniających przez telefon czy Internet. Pracownicy banków czy innych instytucji finansowych nigdy nie będą ich od nas oczekiwali**. Jeśli otrzymujemy np. telefon z informacją, że np. mogło dojść do próby kradzieży środków z naszego rachunku, właściwym postępowaniem w takiej sytuacji jest rozłączenie się i podjęcie samodzielnego kontaktu z Bankiem. Przestępcy podszywają się nie tylko pod pracowników banków, ale również pod pracowników innych instytucji szeroko rozumianego sektora finansowego. Jako przykład można podać sytuację, gdzie osoby nieuprawnione podawały się za pracowników banków podszywając się pod numer telefonu Rzecznika Finansowego – prawa opisana szarzej w komunikacie:

https://rf.gov.pl/2023/08/29/ostrzezenie-przed-proba-podszywania-sie-pod-pracownikow-biura-rzecznika-finansowego/.

Co dalej?

Ochrona klienta przed konsekwencjami zaciągnięcia przez przestępców „kredytu na klik" jest wielowątkowa i koncentruje się na kliku aspektach prawnych.

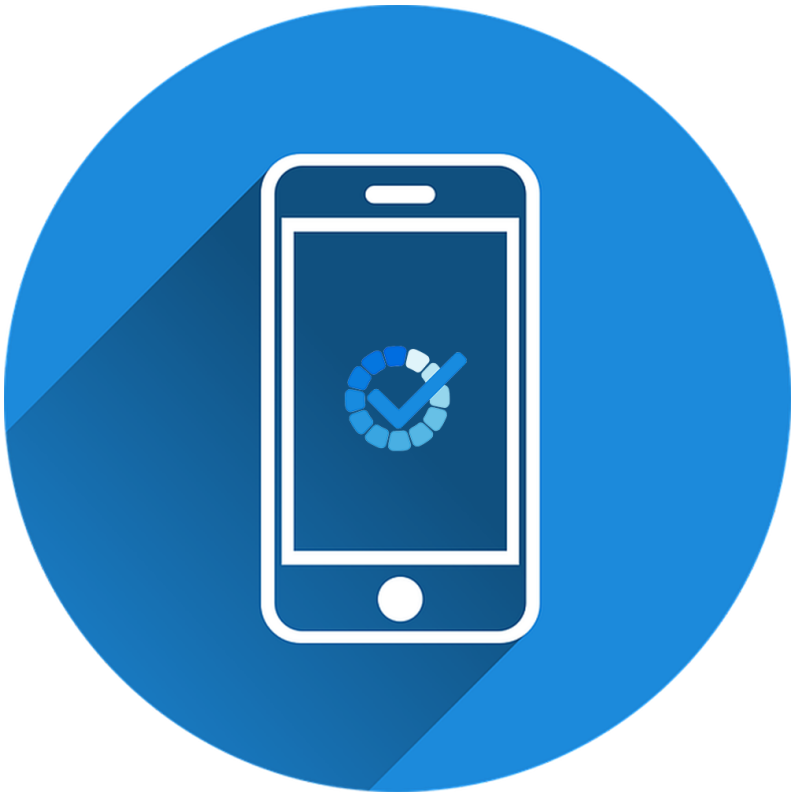
Po pierwsze, Rzecznik Finansowy stoi na stanowisku, że w przypadku wyłudzenia „kredytu na klik" nie można przyjąć, iż zawarta została umowa kredytu między klientem a bankiem. Ktoś, kto nie miał zamiaru złożenia oświadczenia woli i tym samym nie zawarł umowy kredytu świadomie, a zrobił to na skutek oszustwa i manipulacji, nie stanie się osobą, która wskutek działań przestępców takie oświadczenie woli złożyła. W takiej sytuacji Bank został wprowadzony w błąd przez osobę trzecią, która jedynie podszyła się pod klienta.

Drugim narzędziem ochrony klienta są zabezpieczenia wynikające z ustawy o usługach płatniczych. O ile problematyka rzekomego zawarcia umowy „kredytu na klik" między klientem a bankiem nie jest objęta reżimem ustawy o usługach płatniczych, a raczej Kodeksu Cywilnego, o tyle nieautoryzowana wypłata tych środków z rachunku poszkodowanego już taką transakcją będzie. Wiążę się to ze szczególną ochroną tych środków. Polskie prawo w sposób szczególny chroni klientów banków w przypadku utraty środków w związku z nieautoryzowanymi transakcjami płatniczymi, czyniąc banki odpowiedzialnymi za ich skutki, chyba że te wykażą, że klient doprowadził do transakcji umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia obowiązków związanych z korzystaniem z instrumentu płatniczego zgodnie z umową ramową oraz niezwłocznym

zgłaszaniem stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego (art. 46 ust. 3 UUP).

Warto wiedzieć, jak zachować się w sytuacji, gdy padniemy ofiarą wyłudzenia. Najważniejszym jest, aby poszkodowany niezwłocznie poinformował bank o zidentyfikowaniu nieautoryzowanej transakcji płatniczej, czyli np. widocznej jako „oczekująca" w bankowości elektronicznej lub aplikacji mobilnej, ale niezrealizowanego jeszcze zlecenia albo wypłaty środków z rachunku. W konsekwencji powinno dojść do niezwłocznego zablokowania przez bank rachunku w celu zapobieżenia dalszym wypłatom i dokonaniu aktualizacji zabezpieczeń rachunku klienta. Poinformowanie banku może odbyć się różnymi kanałami komunikacji, jednak z uwagi na istotne znaczenie czasu w takich sytuacjach zalecanym jest kontakt telefoniczny. Banki zobowiązane są do udostępnienia infolinii, która umożliwi bezzwłoczny kontakt i możliwość zablokowania rachunku – co wynika wprost z art. 43 ust. 1 pkt 3 ustawy o usługach płatniczych. Jeżeli banki, wbrew wskazanemu obowiązkowi, nie zapewnią odpowiednich środków umożliwiających dokonanie w każdym czasie zgłoszenia o nieautoryzowanej transakcji, klient nie odpowiada za nieautoryzowane transakcje płatnicze, chyba że płatnik doprowadził umyślnie do takich transakcji (art. 46 ust. 5 UUP). Po dokonaniu takiego zgłoszenia klient nie odpowiada za nieautoryzowane transakcje płatnicze – chyba że doprowadził do niej umyślnie (art. 46 ust. 4 UUP).

Warto również pamiętać, że **to na banku** (a nie na kliencie) **spoczywa ciężar udowodnienia, że transakcja płatnicza została autoryzowana i prawidłowo zapisana w systemie** (art. 45 ust. 2 UUP). **Powołanie się przez bank na naruszenia postanowień umowy o świadczenie usług rachunku czy jej załączników (jak np. regulaminu w postaci przekazania przez klienta przestępcom danych służących autoryzacji), o ile nie znajdują one swojego odzwierciedlenia w ustawie, nie stanowi okoliczności wyłączającej odpowiedzialność banku (art. 8 ust. 1 UUP).**



Pomoc Rzecznika Finansowego

W przypadku sporu z bankiem w zakresie wyłudzenia środków poprzez „kredyt na klik" (oraz w sprawie nieautoryzowanych transakcji) w pierwszej kolejności klient powinien złożyć w banku reklamację. Działanie w tym trybie przez klienta umożliwi Rzecznikowi podjęcie interwencji.

Reklamacja to wystąpienie skierowane do podmiotu rynku finansowego przez jego klienta, w którym klient zgłasza zastrzeżenia dotyczące usług świadczonych przez podmiot rynku finansowego. Reklamacja może być złożona w formie pisemnej, ustnej, telefonicznie albo osobiście do protokołu podczas wizyty klienta w jednostce lub w formie elektronicznej z wykorzystaniem środków komunikacji elektronicznej, o ile takie środki zostały do tego celu wskazane przez podmiot rynku finansowego. Zgodnie z art. 3 ustawy o Rzeczniku Finansowym, podmiot rynku finansowego ma obowiązek przyjąć reklamację w każdej swojej jednostce, która obsługuje klientów. Reklamacja złożona zgodnie z określonymi wymogami podlega rozpatrzeniu przez podmiot rynku finansowego w terminie do 15 dni od dnia jej otrzymania (art. 15a UUP).

W przypadku nierozpatrzenia reklamacji zgodnie z oczekiwanymi klienta, zapraszamy do kontaktu z Biurem Rzecznika Finansowego, zakres możliwych działań Rzecznika opisany został szczegółowo pod poniższym linkiem:

https://rf.gov.pl/jak-pomaga-rzecznik-finansowy/

Zmiany w przepisach

Warto także zwrócić uwagę na dwa akty prawne, które dotyczą omawianych kwestii i mają na celu zwiększenie ochrony klientów. Chodzi tu o ustawę z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości oraz ustawę z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

Ustawa z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości, która weszła w życie w dniu 22 lipca 2023 r., ma na celu przede wszystkim zwiększenie ochrony przed nadużyciami wynikającymi z kradzieży danych i ograniczenia skali zjawiska wyłudzania środków finansowych poprzez zaciąganie zobowiązań finansowych na inną osobę (m.in. umowy kredytu, umowy pożyczki, umowy sprzedaży nieruchomości) bez wiedzy i zgody właściciela, a także zjawiska tzw. *SIM swappingu*, czyli wyrobienia duplikatu karty SIM, która może być potem użyta do nielegalnego autoryzowania transakcji.

Przeciwdziałaniu kradzieży tożsamości służyć ma przede wszystkim rozwiązanie przewidziane w art. 8 ustawy, zmieniającym ustawę o ewidencji ludności, które umożliwi osobie, której dane dotyczą, nieodpłatne zastrzeżenie oraz cofnięcie zastrzeżenia numeru PESEL. Zastrzeżenie i cofnięcie zastrzeżenia będzie mogło być dokonane przy użyciu usługi elektronicznej udostępnionej przez ministra właściwego do spraw informatyzacji po uwierzytelnieniu (usługa dostępna na Gov.pl albo za pomocą aplikacji mobilnej mObywatel) albo osobiście do organu dowolnej gminy. Dodatkowo zastrzeżenia numeru PESEL można

dokonać osobiście w banku krajowym, spółdzielczej kasie oszczędnościowo-kredytowej oraz w placówce pocztowej, a także za pomocą systemu teleinformatycznego banku krajowego albo spółdzielczej kasy oszczędnościowo-kredytowej, w którym jest uwierzytelniana osoba dokonująca zastrzeżenia, o ile podmioty te będą świadczyły taką usługę.

Ustawodawca określił również tryb zastrzegania numeru PESEL i cofania zastrzeżenia w przypadku osoby nieposiadającej zdolności do czynności prawnych albo posiadającej ograniczoną zdolność, a także tryb zastrzegania numeru PESEL w przypadku niemożności złożenia wniosku o zastrzeżenie numeru PESEL spowodowanej chorobą, niepełnosprawnością lub inną niedającą się pokonać przeszkodą.

Ponadto minister właściwy do spraw informatyzacji prowadzi rejestr zastrzeżeń numerów PESEL. Rejestr ten będzie prowadzony w systemie teleinformatycznym. Każdy zainteresowany może przy użyciu usługi elektronicznej udostępnionej przez ministra właściwego do spraw informatyzacji nieodpłatnie zweryfikować informację o aktualnym zastrzeżeniu numeru PESEL albo zastrzeżeniu numeru PESEL we wskazanej przez weryfikującego chwili.

W zakresie konieczności weryfikacji (np. przez banki) przez obowiązane podmioty zastrzeżonego numeru PESEL ustawa wejdzie w życie 1 czerwca 2024 r., niemniej sama możliwość jego zastrzegania jest możliwa od dnia 17 listopada 2023 r.

Warto także wspomnieć, że *w projekcie rozporządzenia Parlamentu Europejskiego i Rady w sprawie usług płatniczych na rynku wewnętrznym*[5], ogłoszonym przez Komisję Europejską w dniu 28 czerwca 2023 r., proponuje się m.in. wprowadzić generalną zasadę odpowiedzialności dostawcy usług płatniczych (banku) z tytułu dokonania oszustwa na szkodę konsumenta (i utraty przez niego środków), polegającego na podszywaniu się pod inną osobę, przede wszystkim pracownika danego dostawcy. Proces legislacyjny w tym obszarze trwa, jednak ogłoszenie ww. projektu w zasygnalizowanym wyżej kształcie pozwala na stwierdzenie, że Komisja jest świadoma istotnych wyzwań, które stoją przed ochroną konsumenta w kontekście bezpiecznego korzystania z usług płatniczych na całym rynku unijnym.

Z kolei w ustawie dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej ustawodawca stworzył w prawie krajowym ramy prawne do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej (przewidziano ich otwarty katalog) przez przedsiębiorców telekomunikacyjnych.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367

W tym kontekście nałożono na nich m.in. następujące obowiązki:

- podejmowanie proporcjonalnych środków technicznych i organizacyjnych, mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie;
- podłączenie się do systemu teleinformatycznego przekazującego wzorce wiadomości o charakterze *smishingu*[6] (prowadzonego przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, czyli CSIRT NASK, który będzie monitorował występowanie *smishingu* i przekazywał przedsiębiorcom telekomunikacyjnym omawiane wzorce);
- zapewnienie swoim użytkownikom końcowym oraz CSIRT NASK możliwości bezpłatnego korzystania z numeru 8080, służącego do przekazywania wiadomości do CSIRT NASK, co do których istnieje podejrzenie, że ich treść wyczerpuje znamiona *smishingu*;
- niezwłoczne blokowanie (zautomatyzowane) krótkich wiadomości tekstowych (SMS) zawierających treści zgodne ze wzorcem wiadomości wyczerpującej znamiona *smishingu*;
- blokowanie lub ukrycie identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku wystąpienia *CLI spoofingu* (w sytuacji, gdy prawdopodobieństwo jego wystąpienia jest bardzo wysokie lub wysokie);
- rejestracja danych o usługach telekomunikacyjnych, które nie zostały wykonane z uwagi na blokowanie krótkich wiadomości tekstowych, w zakresie umożliwiającym rozpatrzenie reklamacji.

Ponadto na dostawców poczty elektronicznej (dla co najmniej 500 000 użytkowników lub podmiotu publicznego) nałożono obowiązek stosowania mechanizmów zapobiegających *phishingowi*[7].

Prezes Urzędu Komunikacji Elektronicznej został zobowiązany m.in. do prowadzenia jawnego wykazu numerów służących wyłącznie do odbierania połączeń głosowych. Chodzi tutaj o to, aby połączenie było inicjowane tylko w jednym kierunku przez np. konsumenta, który ze swojego numeru dzwoni na numer infolinii np. banku. Numer ten nie będzie służył do inicjowania połączenia przez bank.

Rozwiązania przyjęte w omawianym akcie prawnym mogą istotnie przyczynić się do ograniczenia liczby oszustw dokonywanych na szkodę klientów z wykorzystaniem metod socjotechnicznych. Tego rodzaju działania oszukańcze (i rosnąca ich skala) stanowią istotne zagrożenie dla prawidłowego funkcjonowania rynku finansowego i zaufania jego uczestników do podmiotów na nim działających. Znaczącą redukcję możliwości posługiwania się przez

[6] Smishing to rodzaj phishingu skierowanego na telefony komórkowe. Celem przestępcy jest zgromadzenie danych osobowych, takich jak na przykład numer ubezpieczenia społecznego lub numer karty kredytowej. Drogą ataku są wiadomości tekstowe lub SMS.
[7] Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

przestępców takimi metodami oszukańczymi, jak *CLI spoofing* czy *phishing* (*smishing*), należy oceniać jako wysoce pożądaną z punktu widzenia ochrony interesów wszystkich podmiotów działających w tym obszarze rynku finansowego.

Ustawa weszła w życie 25 września 2023 r.