KOMISJA NADZORU FINANSOWEGO

DPR-DPRZPW.051.2.2022 Warszawa, 11 sierpnia 2022 r.

Pan
Sebastian Chorąży

Kancelaria Adwokacka
ul. Grzybowska 4 lok. 117
00-131 Kraków

ZAWIADOMIENIE O SPOSOBIE ZAŁATWIENIA PETYCJI

Kierując się treścią art. 13 ust. 1 ustawy z dnia 11 lipca 2014 r. o petycjach (Dz.U. 2018 r., poz. 870 ze zm., dalej: Ustawa o petycjach) w związku z przepisem art. 238 § 1 ustawy z dnia 14 czerwca 1960 r. *Kodeks postępowania administracyjnego* (tekst jedn. Dz.U. z 2021 r., poz. 735 ze zm.) zawiadamiam o negatywnym sposobie załatwienia wniesionej przez Pana petycji z dnia 23 maja 2022 r., zawierającej wniosek : *„o rozważenie podjęcia czynności nadzorczych wobec sektora finansowego,* natomiast w kwestii wniosku cyt. : *„ o podjęcie działań służących prawidłowemu funkcjonowaniu rynku finansowego”* zawiadamiam o pozytywnym sposobie załatwienia wniesionej przez Pana petycji.

UZASADNIENIE

W dniu 23 maja 2022 r. do Komisji Nadzoru Finansowego (dalej: KNF, organ nadzoru, Komisja) wpłynęło Pana wystąpienie, którego przedmiotem było aby Komisja podjęła czynności nadzorcze wobec sektora finansowego, jak również podjęła działania mające na celu prawidłowe funkcjonowanie rynku finansowego. Wskazano także na kluczową rolę działań edukacyjnych prowadzonych wobec klientów banków w zakresie zagrożeń związanych z korzystaniem z bankowości elektronicznej w zakresie oszustw dokonywanych na szkodę klientów banków, wskazano także na pomysły techniczne, jak przeciwdziałać wymienionym w petycji przestępstwom oraz wyrażono nadzieję, że będą one *„przyczynkiem”* do cyt.: „*wydania nowych rekomendacji, a także do wzmocnienia działalności edukacyjnej w omawianym zakresie”.*

Mając na uwadze charakter Pana wystąpienia, wskazać należy, iż zgodnie z art. 2 ust. 3 ustawy o petycjach przedmiotem petycji może być żądanie, w szczególności, zmiany przepisów prawa, podjęcia rozstrzygnięcia lub innego działania w sprawie dotyczącej podmiotu wnoszącego petycję, życia zbiorowego lub wartości wymagających szczególnej ochrony w imię dobra wspólnego, mieszczących się w zakresie zadań i kompetencji adresata petycji.

Tak określony przez ustawodawcę zakres petycji wskazuje, że przedmiotem petycji wniesionej do Komisji Nadzoru Finansowego nie może być żądanie podjęcia określonego działania nadzorczego, jeśli nie mieści się ono w zakresie zadań i kompetencji organu nadzoru.

Mając na uwadze Pana wniosek o *rozważenie podjęcia czynności nadzorczych wobec sektora finansowego* wyjaśnić należy, iż zgodnie z art. 2 ustawy z dnia 21 lipca 2006 r. *o nadzorze nad rynkiem finansowym* (t.j. Dz. U. z 2022 r. poz. 660 z późn. zm.; dalej: ustawa o nadzorze): *„celem nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku również poprzez rzetelną informację dotyczącą funkcjonowania rynku, przez realizację celów określonych w szczególności w ustawie - Prawo bankowe, (...)”.*

Przy czym cel ten może być realizowany poprzez wskazane w art. 133 ust. 1 ustawy z dnia 29 sierpnia 1997 r. – *Prawo bankowe* (Dz. U. z 2021 r. poz. 2439, dalej: ustawa Prawo bankowe) „czynności podejmowane w ramach nadzoru bankowego, które polegają w szczególności na:

1) dokonywaniu oceny sytuacji finansowej banków, w tym badaniu wypłacalności, jakości aktywów, płynności płatniczej, wyniku finansowego banków;

2) badaniu jakości systemu zarządzania bankiem, w szczególności systemu zarządzania ryzykiem oraz systemu kontroli wewnętrznej;

3) badaniu zgodności udzielanych kredytów, pożyczek pieniężnych, akredytyw, gwarancji bankowych i poręczeń oraz emitowanych bankowych papierów wartościowych z obowiązującymi w tym zakresie przepisami;

4) badaniu zabezpieczenia i terminowości spłaty kredytów i pożyczek pieniężnych;

5) badaniu przestrzegania limitów, o których mowa w art. 79a, oraz limitów, o których mowa w art. 395 rozporządzenia nr 575/2013, oraz ocenie procesu identyfikacji, monitorowania i kontroli koncentracji ekspozycji, w tym dużych ekspozycji;

6) badaniu przestrzegania przez bank, określonych przez Komisję Nadzoru Finansowego norm dopuszczalnego ryzyka w działalności banków, zarządzania ryzykiem prowadzonej działalności, w tym dostosowania do rodzaju i skali działalności banku procesu identyfikacji i monitorowania ryzyka oraz sprawozdawania o ryzyku;

7) dokonywaniu oceny szacowania, utrzymywania i przeglądu kapitału wewnętrznego;

8) badaniu wykonywania przez banki obowiązków, o których mowa w art. 56a, art. 59a, art. 59b, art. 92ba-92bd i art. 111c.

Powyższe oznacza, że cele nadzoru finansowego realizowane są poprzez dokonywanie oceny generalnych zasad ograniczania ryzyka związanego z działalnością banków, jakości zarządzania, adekwatności kapitałów i poprawności stosowanych procedur.

Zakres możliwych działań Komisji Nadzoru Finansowego określają przepisy art. 137 i 138 ust. 1 ustawy *Prawo bankowe*. Zgodnie z art. 137 ustawy *Prawo bankowe*, Komisja Nadzoru Finansowego może wydawać rekomendacje dotyczące dobrych praktyk ostrożnego i stabilnego

zarządzania bankami. Zgodnie zaś z art. 138 ust. 1 ustawy *Prawo bankowe* Komisja Nadzoru Finansowego może w ramach nadzoru zalecić bankowi w szczególności:

1) podjęcie środków koniecznych do przywrócenia płynności płatniczej lub osiągnięcia i przestrzegania norm dopuszczalnego ryzyka w działalności banku;
2) zaniechanie określonych form reklamy;
3) opracowanie i stosowanie procedur, które zapewnią utrzymywanie, bieżące szacowanie i przegląd kapitału wewnętrznego oraz funkcjonowanie systemu zarządzania bankiem;
4) zastosowanie szczególnych zasad tworzenia rezerw na ryzyko związane z działalnością banków lub odpisów z tytułu utraty wartości aktywów lub szczególnego traktowania aktywów przy obliczaniu wymogów w zakresie funduszy własnych;
5) ograniczenie ryzyka występującego w działalności banku, w tym ryzyka wynikającego z powierzenia wykonywania czynności, o którym mowa w art. 6a ust. 1; str. 4
6) ograniczenie wysokości zmiennego składnika wynagrodzenia osób objętych polityką wynagrodzeń, jako odsetka przychodów netto, w przypadku gdy jego wysokość utrudnia spełnianie wymogów w zakresie funduszy własnych;
7) wypełnianie dodatkowych obowiązków sprawozdawczych lub zwiększenie ich częstotliwości, w tym sprawozdawczości w zakresie funduszy własnych, płynności i dźwigni finansowej, o ile obowiązki te są adekwatne do celu, w jakim są nakładane;
8) ujawnianie dodatkowych informacji;
9) przestrzeganie art. 92ba-92bd oraz art. 111c ustawy Prawo bankowe.

Wyjaśnienia przy tym także wymaga, że nadzór sprawowany przez Urząd KNF nad sektorem bankowym w Polsce ma charakter nadzoru systemowego i ostrożnościowego, zaś wskazane wyżej cele, katalog form działań nadzorczych oraz możliwe do podjęcia środki wyznaczają jednocześnie granice dozwolonej prawem ingerencji organu nadzoru finansowego w działalność banków, jako niezależnych podmiotów prawa.

Dla realizacji powyższego celu nadzoru bankowego, KNF analizuje szereg informacji dotyczących działalności banków, w tym także informacji dotyczących nieprawidłowości przesyłanych przez klientów banków.

Jednocześnie zauważyć należy, iż informacje dotyczące podmiotów nadzorowanych mogą być podstawą postępowania wszczynanego przez KNF z urzędu i mającego na celu wydanie przewidzianego prawem rozstrzygnięcia nadzorczego.

Natomiast działania nadzorcze podejmowane przez Urząd KNF w stosunku do podmiotów nadzorowanych nie mają bezpośredniego wpływu na rozstrzygnięcie spraw indywidualnych. Działania te realizowane są urzędu, zaś przyczyną ich podjęcia jest ustawowy obowiązek sprawowania nadzoru przez Komisję Nadzoru Finansowego, a nie wniosek osoby zainteresowanej.

Tym samym wniesiona przez Pana petycja w zakresie cyt. : „*rozważenie podjęcia czynności nadzorczych wobec sektora finansowego”* nie może zostać załatwiona w sposób pozytywny.

Jednocześnie podkreślenia wymaga, iż otrzymana korespondencja potraktowana zostanie jako zgłoszenie o dostrzeżonych nieprawidłowościach i poddane ono zostanie także stosownej analizie pod kątem ww. celów oraz kompetencji Komisji Nadzoru Finansowego.

Natomiast analiza otrzymywanych zgłoszeń polega na stałym monitorowaniu praktyk rynkowych, jak i na działaniach interwencyjnych, szczególnie w tych obszarach działalności nadzorowanych podmiotów, w których mogą występować naruszenia prawa lub interesów nieprofesjonalnych uczestników rynku finansowego.

W kwestii dotyczącej podjęcia przez Komisję działań mających na celu prawidłowe funkcjonowanie rynku finansowego, poprzez cyt. : „*wydania nowych rekomendacji, a także do wzmocnienia działalności edukacyjnej w omawianym zakresie* zauważyć należy, iż w zakresie poruszanej przez Pana problematyki oszustw metodą *„na telefon z banku”* dokonywanych na szkodę klientów banków, w tym z wykorzystaniem *spoofingu* są obecnie stosowane rozwiązania technologiczne mogące jedynie ograniczyć skalę tego zjawiska, które uderza nie tylko w sektor finansowy, natomiast nie umożliwiają one jednak jego eliminacji.

Wśród wykorzystywanych obecnie metod ograniczania *spoofingu* telefonicznego należy wskazać zastosowanie zdefiniowanego przez klienta hasła lub weryfikacji w aplikacji mobilnej. Pierwszy z wymienionych sposobów polega na podaniu znanego klientowi dedykowanego hasła przez pracownika banku inicjującego kontakt. Rozwiązania polegające na stosowaniu hasła lub weryfikacji w aplikacji mobilnej cechuje bezpieczeństwo, nie są one jednak łatwe do stosowania z perspektywy klienta oraz banku ze względu na fakt, że kontakt z infolinią banku następuje sporadycznie, a klienci mają trudności z zapamiętaniem ustalonego hasła, dedykowanego weryfikacji pracownika banku nawiązującego kontakt.

Weryfikacja w aplikacji mobilnej zakłada powiadomienie przez bank, poprzez wiadomość *„push”* wysyłaną do aplikacji mobilnej klienta banku, o połączeniu telefonicznym realizowanym przez bank do tego klienta. Część banków posiada już rozwiązanie tego typu, a zgodnie z informacjami posiadanymi przez organ nadzoru, kolejne banki uruchamiają je dla swoich klientów.

Natomiast w przypadku potwierdzenia w aplikacji mobilnej, to potencjalna skala zastosowania omawianego rozwiązania ograniczona jest do użytkowników aplikacji mobilnej danego banku, a jednocześnie wymagana jest w tym zakresie umiejętność korzystania z aplikacji podczas prowadzonej rozmowy telefonicznej, co może utrudniać zastosowanie omawianego rozwiązania np. w przypadku pewnych grup odbiorców korzystających z bankowości mobilnej.

Problem *spoofingu* telefonicznego został dostrzeżony na poziomie państwa polskiego, które podjęło działania mające na celu wyeliminowanie tego zagrożenia.

W styczniu bieżącego roku, pilne wprowadzenie rozwiązań chroniących przed *spoofingiem* telefonicznym, we współpracy z rynkiem telekomunikacyjnym, zapowiedział Pan Janusz Cieszyński, Pełnomocnik Rządu ds. Cyberbezpieczeństwa. Zgodnie z zapowiedzią, projektowane rozwiązania miałyby na celu specjalne oznaczenie połączeń przychodzących w ramach *spoofingu* telefonicznego, aby użytkownik mógł je odróżnić od połączenia pochodzącego od osoby uprawnionej do korzystania z danego numeru telefonu[1]. 14 czerwca

2022 r. do wykazu prac legislacyjnych i programowych Rady Ministrów wprowadzony został *„Projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej”*[2]. Urząd KNF bierze udział w pracach mających na celu wdrożenie w/w rozwiązania.

W ocenie organu nadzoru rozwiązania technologiczne umożliwiające zwalczanie *spoofingu* telefonicznego korzystnie wpłyną również na bezpieczeństwo klientów sektora finansowego, jednak Komisja Nadzoru Finansowego niezależnie od przedstawionych wyżej planowanych zmian prawnych i technologicznych, podejmuje szereg innych działań mających na celu ochronę klientów usług finansowych.

Działalność Urzędu KNF w omawianym zakresie skupia się na edukacji oraz rozwijaniu świadomości cyberzagrożeń wśród klientów usług finansowych. Uwzględniając fakt, że istotnym elementem *modus operandi* cyberprzestępców *„podszywających się”* pod banki w celu wyłudzania środków finansowych jest socjotechnika, w ocenie KNF to właśnie edukacja pozostaje podstawowym środkiem zapobiegania negatywnym konsekwencjom omawianych zjawisk. W przypadku ataków opartych o manipulowanie ofiarą, to od jej świadomości cyberzagrożeń, rozpoznawania ich oraz reagowania na nie w odpowiedni sposób, zależy w dużej mierze bezpieczeństwo posiadanych przez nią środków.

Działania edukacyjno-informacyjne Urzędu KNF w zakresie przestrzegania przed zagrożeniami w sieci, w tym przed podszywaniem się pod inne banki i inne instytucje oraz firmy, a także z obszaru cyberbezpieczeństwa i zarządzania bezpieczeństwem w obszarze teleinformatycznym, czy też przestrzegania przed działaniem oszustów nakłaniających do inwestowania poprzez platformy inwestycyjne, skierowane do różnych grup odbiorców, wpisane są w misję i cele ustawowe Urzędu KNF a realizowane są w szczególności poprzez:

1. organizację spotkań, na których prezentowane są zagadnienia cyberbezpieczeństwa usług finansowych – w 2021 r. zorganizowanych zostało 12 spotkań z udziałem 3716 uczestników;
2. organizację szkoleń dla organów ścigania oraz wymiaru sprawiedliwości, w tym w 2019 r. szkolenie „*Cyberbezpieczeństwo sektora finansowego. Aspekty systemowe i praktyka przeciwdziałania cyberprzestępczości”;* w 2020 r. szkolenie „*Cyberbezpieczeństwo sektora finansowego z perspektywy rynku i klienta. Aspekty systemowe i profilaktyka przeciwdziałania cyberprzestępczości”;*a także w 2021 r. szkolenia *„Cyberbezpieczeństwo usług finansowych”* oraz „*Metody ataków na środki finansowe klientów bankowości internetowej, stosowane przez cyberprzestępców”;*

---

[1] 1 https://cyberdefence24.pl/cyberbezpieczenstwo/cieszynski-chcemy-pilnie-wprowadzic-rozwiazaniachroniaceprzed-spoofingiem-i-phisingiem

[2] https://www.gov.pl/web/premier/projekt-ustawy-o-zwalczaniu-naduzyc-w komunikacjielektronicznej?fbclid=IwAR2OdVkq_cLVHdUyhOIt3sXQyNDsbsLNbEXHfsvIbBff9akLksZysfIXj8

3. publikację ostrzeżeń w mediach społecznościowych (Twitter, Facebook), odnoszących się do zagrożeń cyberbezpieczeństwa – w 2021 r. opublikowano 159 takich ostrzeżeń,

które to ostrzeżenia są następnie publikowane przez poczytne media o zasięgu krajowym;

4. publikację opracowań oraz artykułów dotyczących zagadnień cyberbezpieczeństwa usług finansowych – w 2021 r. opublikowano 10 opracowań oraz 5 artykułów w prasie tradycyjnej o skali ogólnopolskiej.

Zgodnie z powyższym szczególnie uwzględnić należy:

a) kampanię informacyjną UWAGA CYBEROSZUST na temat oszustw z wykorzystaniem dokumentów opatrzonych logiem KNF/UKNF lub osób powołujących się na KNF. Partnerem Kampanii była Komenda Główna Policji a kampania zainaugurowana została pod koniec 2020 r. i kontynuowana w 2021 r. ;

b) w marcu 2021 r. na antenie Radia Zet oraz RMF FM, zostały wyemitowane spoty ostrzegające przed cyberoszustami. Wspólnie z Policją, Urząd KNF przybliżał metody działań przestępców, a także uświadamiał klientom sektora finansowego możliwe zagrożenia i ryzyka. Kampania miała za zadanie wskazać mechanizmy, jakie wykorzystują oszuści w procederze wyłudzania pieniędzy m.in. podczas pośrednictwa wymiany kryptowalut, czy przy fałszywych działaniach podejmowanych rzekomo przez KNF lub Urząd KNF;

c) w ramach minicyklu publikacji w dziennikach regionalnych, zamieszczano artykuły przygotowywane przez CSIRT KNF o wszelkiego rodzaju oszustwach internetowych, czy telefonicznych;

d) inicjatywy zrealizowane przez Urząd KNF w ramach projektu edukacyjnego *Centrum Edukacji dla Uczestników Rynku - CEDUR* w 2021 r. oraz w okresie od stycznia do maja 2022 r.;

e) podcasty zrealizowane przez Urząd KNF – *Finanse pod nadzorem*[1]:

- podcast pt.: *Cyberbezpieczeństwo – jak działają przestępcy?* - w odcinku podcastu przedstawiciele Urzędu KNF wyjaśniają sposoby działania cyberprzestępców. Szczególnie zwracają uwagę m.in. na podszywanie się pod przedstawicieli instytucji publicznych, firmy kurierskie, a także na oszustów działających na popularnych portalach sprzedażowych i w mediach społecznościowych. Materiał dostępny pod adresem: https://www.knf.gov.pl/komunikacja/podcast/cyberbezpieczenstwo?articleId=7624
6&p_id=18
- podcast pt.: *Jak przestępcy podszywają się pod KNF i UKNF? - w* odcinku podcastu przedstawiciele Urzędu KNF wyjaśniają jak oszuści powołują się na

[1] *Finanse pod nadzorem* to cykl nagrań o charakterze edukacyjnym, odnoszących się do zagadnień z zakresu rynku finansowego. Podcast UKNF skierowany jest przede wszystkim do nieprofesjonalnych uczestników rynku finansowego, w szczególności obecnych i przyszłych klientów, konsumentów. Celem tego Programu jest podniesienie poziomu wiedzy nt. rynku finansowego, umożliwiające podejmowanie świadomych decyzji na rynku finansowym. W każdym odcinku podcastu eksperci z UKNF omawiają wybrane zagadnienia, wyjaśniają na co warto zwracać uwagę, by świadomie zarządzać swoimi finansami. Wskazują potencjalne ryzyka i zagrożenia, a także poruszają kwestie, które powinny wzbudzić czujność.

KNF i UKNF i jakie dane próbują wtedy pozyskać, jakie metody stosują i jak nie dać się oszukać, a także gdzie może zgłosić się osoba poszkodowana i jak chronić swoje dane. Materiał dostępny pod adresem:
https://www.knf.gov.pl/komunikacja/podcast/jak_przestepcy_podszywaja_sie_pod_KNF_i_UKNF?articleId=77152&p_id=18;

- podcast pt.: *Platformy inwestycyjne – co musisz wiedzieć zanim zainwestujesz?* - w odcinku podcastu przedstawiciele Urzędu KNF wyjaśniają, czym są platformy inwestycyjne i co zrobić, by nie dać się oszukać. Materiał dostępny pod adresem: https://www.knf.gov.pl/komunikacja/podcast/platformy_inwestycyjne?articleId=76131&p_id=18;

f) webinaria CEDUR[2] dla różnych grup odbiorców, m.in. środowiska szkolnego, seniorów oraz podmiotów podlegających nadzorowi KNF, m.in.:

- webinaria dla środowiska szkolnego:

- dwa webinaria pt. *Cyberoszuści atakują - jak nie dać się okraść w Internecie*: terminy realizacji 24 marca 2021 r. oraz 23 marca 2022 r. zorganizowane w ramach kampanii Global Money Week (dalej: GMW)[3] oraz warsztaty edukacyjne z zakresu cyberbezpieczeństwa usług finansowych dla młodzieży. Materiały z webinariów dostępne pod adresem:
https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=72703&p_id=18 oraz
https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=77338&p_id=18;
- webinar pt. *Oszustwa na rynku finansowym dlaczego wciąż im ulegamy*, termin realizacji 25 marca 2021 r., zorganizowane w ramach kampanii GMW.
Materiały dostępne pod adresem:
https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=72699&p_id=18;
- webinar pt.: *Cyberbezpieczeństwo z perspektywy klienta usług finansowych – aspekty praktyczne*, termin realizacji 5 października 2021 r. zorganizowane w ramach WIW[4].
Materiały dostępne pod adresem:

[2] Webinaria organizowane w ramach projektu edukacyjnego *Centrum Edukacji dla Uczestników Rynku - CEDUR* prowadzone są głównie przez pracowników Urzędu KNF. Udział w webinariach jest bezpłatny.

[3] GMW - międzynarodowa kampania Global Money Week – Światowy Tydzień Pieniądza, której organizatorem jest Międzynarodowa Sieć ds. Edukacji Finansowej działająca przy Organizacji Współpracy Gospodarczej i Rozwoju - OECD/INFE. UKNF jest koordynatorem kampanii GMW na gruncie krajowym.

[4] WIW - kampania o zasięgu globalnym powołana do życia przez Międzynarodową Organizację Komisji Papierów Wartościowych (IOSCO) w 2017 r. na rzecz zwiększenia świadomości społecznej na temat roli edukacji oraz ochrony inwestorów na rynku finansowym.

https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=74797&p_id=18;

- webinar pt.: *Bezpieczny telefon jak chronić się przed cyberprzestępcami*, termin realizacji 25 marca 2021 r., zorganizowane w ramach kampanii GMW. Materiały odstępne pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=77323&p_id=18;
- wykład/prezentacja *„Sposoby kradzieży środków finansowych w cyberprzestrzeni Jak nie dać się okraść w Internecie,* termin realizacji 15 marca 2022 r. zorganizowany w ramach odchodów światowego dnia konsumenta;
- przedstawienie zagadnień ochrony informacji w cyberprzestrzeni w ramach panelu konferencji POLSECURE, a także zagadnień relacji między cyberbezpieczeństwem a bezpieczeństwem fizycznym w ramach panelu *„Nowe wyzwania regulacyjne i nadzorcze w obszarze innowacji finansowych"* na Uniwersytecie Warszawskim;
- szkolenia z zakresu cyberbezpieczeństwa usług finansowych dla uczniów szkół średnich;
- przedstawienie zagadnień edukacji z zakresu cyberbezpieczeństwa w ramach panelu konferencji z okazji Międzynarodowego Dnia Dziecka *„Bezpieczny dzieciak w cyber"* na Uniwersytecie Warszawskim;

b) webinaria dla podmiotów podlegających nadzorowi KNF:

- *Zarządzanie obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w SKOK*, termin realizacji 17 czerwca 2021 r. (skierowane do spółdzielczych kas oszczędnościowo-kredytowych). Materiały dostępne pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=73717&p_id=18;
- *Cyberbezpieczeństwo*, termin realizacji 5 listopada 2021 r. (skierowane do banków spółdzielczych). Materiały dostępne pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=75307&p_id=18;
- *Zarządzanie obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach rynku finansowego – wymagania wobec banków*, termin realizacji 9 listopada 2021 r. (skierowane do banków komercyjnych). Materiały dostępne pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=75657&p_id=18;
- *Cyberbezpieczeństwo w sektorze ubezpieczeniowym*, termin realizacji 19 listopada 2021 r. (skierowane do zakładów ubezpieczeń i zakładów reasekuracji). Materiały dostępne pod adresem:

https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=75712&p_id=18;

c) webinaria dla innych grup odbiorców:

- *Cyberbezpieczeństwo w sektorze banków i ubezpieczycieli*, realizacja 25 maja 2021 r. (skierowane do biegłych rewidentów). Materiał dostępny pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=73503&p_i d=18;
- *Cyberbezpieczeństwo sektora finansowego z perspektywy rynku i klienta. Aspekty systemowe i profilaktyka przeciwdziałania cyberprzestępczośc*i, termin realizacji 24 września 2021 r. (skierowane do instytucji ochrony praw nieprofesjonalnych uczestników rynku finansowego, w tym do miejskich i powiatowych rzeczników konsumentów). Materiały dostępne pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=74587&p_i d=18; ○ *Cyberoszuści atakują - jak nie dać się okraść w Internecie*, termin realizacji 28 kwietnia 2022 r. (skierowane do seniorów, zorganizowane we współpracy z Komendą Główną Policji). Materiały dostępne pod adresem:

https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=77681&p_id=18;

- *Zarządzanie bezpieczeństwem w obszarze teleinformatycznym*, termin realizacji 7 czerwca 2022 r. (skierowane do spółdzielczych kas oszczędnościowokredytowych). Materiały dostępne pod adresem:

https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=78074&p_i d=18;

- *Zarządzanie obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego*, termin realizacji 28 czerwca 2022 r. (skierowane do podmiotów sektora usług płatniczych). Materiały dostępne pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=78244&p_i d=18;
- *Nieautoryzowane transakcje płatnicze. Cyberbezpieczeństwo podczas zawierania transakcji elektronicznych z podmiotami rynku finansowego*, termin realizacji 29 czerwca 2022 r. (skierowane do instytucji ochrony praw nieprofesjonalnych uczestników rynku finansowego, w tym do miejskich i powiatowych rzeczników konsumentów). Materiały dostępne [pod adresem: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=78012&p_i d=18.
- prezentacja zagadnień dot. zagrożeń dla klientów bankowości spółdzielczej w ramach konferencji „*Czerwiec z bankiem spółdzielczym";*
- *prezentacja pt. „Bezpieczne finanse – czyli jak nie dać się okraść w cyberprzestrzeni"* w ramach konferencji Sacroexpo

Ponadto w ramach projektu CEDUR zaplanowano do realizacji w okresie od lipca do grudnia 2022 r. m.in. następujące webinaria, skierowane do różnych grup odbiorców: ○ *Problematyka i profilaktyka cyberbezpieczeństwa w bankach spółdzielczych* (skierowane do banków spółdzielczych); ○ *Jak nie dać się okraść w Internecie – przedstawienie na praktycznych przykładach sposobów działania cyberprzestępców oraz dobrych praktyk, które umożliwią bezpieczną realizację płatności w Internecie* (skierowane do środowiska szkolnego);

- *Jak zadbać o bezpieczeństwo swojego telefonu i nie dać się okraść* (skierowane do środowiska szkolnego);
- dwa webinaria pt. *Cyberbezpieczeństwo z perspektywy klienta usług finansowych – aspekty praktyczne* (skierowane odrębnie do środowiska szkolnego oraz seniorów);
- pięć webinariów pt. *DORA i inne regulacje dotyczące obszaru technologicznego okiem organu nadzoru. Wymagania Rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego. Najlepsze praktyki zarządzania incydentami środowiska teleinformatycznego* (skierowanych odrębnie do banków komercyjnych, banków spółdzielczych, spółdzielczych kas oszczędnościowo-kredytowych, podmiotów ryku kapitałowego, podmiotów rynku ubezpieczeniowego).

W nawiązaniu do powyższego szczególnego podkreślenia przy tym wymaga, że w ramach Urzędu KNF działa także Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (dalej: „CSIRT KNF"), prowadzący aktywną działalność edukowania i budowania świadomości cyberbezpieczeństwa w zakresie korzystania z usług finansowych.

Na podstawie artykułów i ostrzeżeń opublikowanych przez CSIRT KNF w 2021 r. powstały 1102 artykuły w portalach branżowych oraz informacyjnych o szerokim zasięgu społecznym, jak www.onet.pl, www.bankier.pl, www.money.pl, www.tvn24.pl, www.biznes.wprost.pl, www.polskatimes.pl, czy www.msn.com. Informacje bazujące na artykułach CSIRT KNF były publikowane także przez media tradycyjne jak Radio Zet, RMF FM, czy Polskie Radio.

Przejawem aktywności KNF w omawianym obszarze edukacji było również zorganizowanie i utrzymywanie portalu dedykowanego m.in. podnoszeniu świadomości klientów rynku finansowego w zakresie zagrożeń – Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego[5] (CEBRF).

Obok Encyklopedii Cyberbezpieczeństwa, można na nim odnaleźć także inne materiały edukacyjne, w tym listę rekomendacji bezpiecznego korzystania z usług finansowych w sieci, quiz dotyczący wiadomości *phishingowych* oraz serię artykułów poświęconych przede wszystkim bieżącym zagrożeniom w cyberprzestrzeni.

Dodatkowo warto także wspomnieć o uruchomieniu przez Urząd KNF platformy edukacyjnej Fintech prowadzonej pod adresem https://fintech.gov.pl/pl/, która służy do komunikacji z

[5] https://cebrf.knf.gov.pl/

sektorem innowacji finansowych (FinTech). Na ww. stronie można również znaleźć zbiór kursów, który został przygotowany w ramach kampanii edukacyjnej, mającej na celu przekazanie oraz pogłębienie wiedzy o rynku finansowym.

W poszczególnych kursach w optymalny sposób wyjaśnione zostały zasady funkcjonowania oraz możliwości, jakie dają innowacyjne rozwiązania na rynku usług bankowych, jak również zagadnienia, z którymi warto się zapoznać by w świadomy i bezpieczny sposób z nich korzystać.

Działania w zakresie zwiększenia świadomości cyberzagrożeń wśród klientów rynku finansowego są podejmowane także przez same banki w związku z wymaganiami stawianymi bankom przez KNF w *„Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach"* a w szczególności w rekomendacji 16.8.

Należy przy tym wskazać, że intensyfikacja działań banków w obszarze edukacji klientów nastąpiła w szczególności po sformułowaniu oczekiwania nadzoru, które wyrażone zostało w piśmie Przewodniczącego Komisji Nadzoru Finansowego do sektora bankowego[6] . Wskazano w nim, że kwestia edukacji i świadomość w obszarze cyberbezpieczeństwa są jednym z gwarantów bezpieczeństwa środków finansowych klientów i powinny być nadal adresowane przez dostawców usług bankowych.

Jednakże za niewystarczające nadzór uznał działania edukacyjne ograniczone do publikowania informacji na stronach internetowych, wyrażając jednocześnie oczekiwanie podejmowania działań edukacyjnych i kampanii medialnych wykraczających poza działania adresowane tylko do swoich klientów, jak np. organizacja ogólnodostępnych szkoleń, aktywny udział w procesie edukacji, czy prowadzenie w mediach tradycyjnych kampanii społecznych budujących kulturę cyberbezpieczeństwa.

W petycji wskazano także na rozwiązania wykraczające poza aspekt edukacyjny, które Pana zdaniem mogłyby rozwijać banki, w celu zapewnienia dodatkowej ochrony swoim klientom. Miałyby one opierać się przy tym w dużej mierze na wykorzystaniu informacji o charakterze behawioralnym, opartych na wzorcach zachowania klienta.

Należy przy tym wskazać, że rozwiązania z zakresu przeciwdziałania oszustwom, polegające na bieżącym monitorowaniu transakcji i zachowania klienta korzystającego z bankowości elektronicznej, są przez banki stosowane zgodnie z przepisami europejskimi. Omawiane wymogi przewidują posiadanie przez dostawców usług płatniczych mechanizmów monitorowania transakcji, które umożliwiają im minimalizowanie ryzyka występowania nieautoryzowanych lub nielegalnych transakcji płatniczych.

[6] Cyberbezpieczeństwo elektronicznych kanałów dostępu do usług bankowych – list Przewodniczącego KNF do sektora bankowego, 15 lutego 2021 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Cyberbezpieczenstwo_elektronicznych_kanalow_dostepu_do_uslug_bankowych%E2%80%93list_Przewodniczacego_KNF_do_sektora_bankowego_72587.pdf

W mechanizmach tych uwzględnia się przy tym analizę transakcji płatniczych z uwzględnieniem elementów, które są typowe dla danego użytkownika usług płatniczych w warunkach zwykłego stosowania indywidualnych danych uwierzytelniających[7].

Ponadto, kwestia funkcjonowania systemów monitorujących transakcje płatnicze, w celu zapewnienia ich bezpieczeństwa, była również przedmiotem rekomendacji KNF, w których wskazano m.in., że *„Dostawcy usług płatniczych powinni stosować mechanizmy monitorowania transakcji mające na celu zapobieganie nielegalnym/oszukańczym transakcjom oraz wykrywanie i blokowanie takich transakcji płatniczych przed wykonaniem przez dostawcę usługi płatności internetowej."*[8].

Banki rozwijają przy tym stale omawiane systemy dostosowując ich funkcjonalności zarówno do dokonywanej analizy ryzyka i charakteru działalności, z uwzględnieniem nowych technik ataków stosowanych przez cyberprzestępców i wynikających z tego zagrożeń. Kwestie implementacji rozwiązań biometrii behawioralnej do systemów ochrony klientów są obecnie na etapie analiz prowadzonych przez podmioty rynku finansowego.

Uwzględniając zarysowaną powyżej istotną wagę edukacji oraz rozwiązań technologicznych dla zapewnienia bezpieczeństwa klientów usług finansowych, jak również mając na uwadze postulaty zawarte w petycji, Urząd KNF będzie kontynuować działania edukacyjne oraz nadzorcze, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa klientów na rynku usług finansowych, a w szczególności usług płatniczych.

Kampanie uświadamiające klientów usług finansowych w zakresie oszustw dokonywanych za pomocą środków porozumiewania na odległość prowadzone są od dawna przez Urząd KNF oraz inne organy publiczne, zrzeszenia konsumenckie, izby gospodarcze podmiotów aktywnych na rynku finansowym, ośrodki naukowe i szkoleniowe.

Inicjatywy przeciwdziałania cyberzagrożeniom i przestępstwom na rynku finansowym dokonywanym na szkodę instytucji finansowych i ich klientów podejmowane są przez Urząd KNF zwłaszcza w ramach obszaru cyberbezpieczeństwa, a zagadnienia będące przedmiotem wniesionej przez Pana petycji nie są obce także organom ścigania i administracji rządowej.

W świetle powyższych wyjaśnień informuję, iż Pana petycja w zakresie wniosku cyt.: „ *o podjęcie działań służących prawidłowemu funkcjonowaniu rynku finansowego"* została załatwiona w sposób pozytywny.

POUCZENIE

Zgodnie z przepisem art. 13 ust. 1 Ustawy o petycjach sposób załatwienia petycji nie może być przedmiotem skargi.

[7] Art. 2 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.

[8] Komisja Nadzoru Finansowego – Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo – kredytowe, Warszawa, listopad 2015 r., rekomendacja 10.

Z upoważnienia
Komisji Nadzoru Finansowego

[redacted]

/podpisano kwalifikowanym podpisem elektronicznym/

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „RODO", informujemy, że:

1. *Administratorem Pana danych osobowych jest Komisja Nadzoru Finansowego (KNF) z siedzibą w Warszawie (00-549), przy ul. Pięknej 20. Z KNF można się kontaktować pisemnie, kierując korespondencję na adres: ul. Piękna 20, skr. poczt. nr 419, 00-549 Warszawa lub pocztą elektroniczną na adres: knf@knf.gov.pl*
2. *Komisja Nadzoru Finansowego zapewnia kontakt z Inspektorem Ochrony Danych (IOD). Z IOD można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych, w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem poprzez adres mailowy: iod@knf.gov.pl lub pisemnie na adres korespondencyjny administratora. Dane IOD znajdują się na stronie internetowej KNF pod adresem: https://www.knf.gov.pl/o_nas/urzad_komisji/dane_teleadresowe*
3. *Pana dane osobowe będą przetwarzane w celu związanym ze zgłoszoną informacją o nieprawidłowościach w zakresie podejmowania przez KNF działań służących prawidłowemu funkcjonowaniu rynku finansowego. Podstawą prawną przetwarzania jest art. 6 ust. 1 lit. e) RODO, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, w związku z art. 4 ust. 1 pkt 2 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (tj. Dz.U. z 2022 r. poz. 660, z późn. zm.) oraz art. 2 ustawy z dnia z dnia 11 lipca 2014 r. o petycjach (tj. Dz.U z 2018 r. poz. 870).*
4. *Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celu, o którym mowa w pkt 3, z zastrzeżeniem przepisów archiwizacyjnych określających okres przechowywania dokumentacji w Urzędzie Komisji Nadzoru Finansowego.*
5. *Pana dane mogą być przekazane do podmiotów, których dotyczy złożona przez Pana informacja o nieprawidłowościach, chyba, że nie wyraził Pan na to zgody.*
6. *Pana dane osobowe nie będą przekazywane innym niż wskazane w pkt 5 podmiotom, w tym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, z wyjątkiem organów publicznych, dla których podstawę prawną udostępnienia stanowi przepis prawa.*
7. *Przysługuje Panu prawo żądania dostępu do danych osobowych, sprostowania, ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania.*
8. *W przypadku gdy uzna Pan, że przetwarzanie danych osobowych narusza przepisy prawa przysługuje Panu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.*
9. *Podanie danych osobowych jest dobrowolne, ale niezbędne dla realizacji celu, o którym mowa w pkt 3.*