



KOMISJA NADZORU FINANSOWEGO

Przewodniczący
Andrzej Jakubiak

DPP – WOP1/023/271/8/13/AJ

Warszawa, 2013-05-13

Pan
Wojciech R. Wiewiórowski
Generalny Inspektor Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

W odpowiedzi na pismo nr GI-035-3/13/1680 z dnia 14 marca 2013 r. w sprawie problematyki funkcjonowania kart zbliżeniowych, przedstawiam poniżej stanowisko Urzędu Komisji Nadzoru Finansowego.

Udzielając odpowiedzi na przywołane powyżej pismo, chciałbym zwrócić uwagę na następujące kwestie: (1) zakres właściwości Urzędu KNF, (2) uregulowania prawne płatności kartami zbliżeniowymi oraz rekomendacji D Komisji Nadzoru Finansowego (3) działania Urzędu KNF w kwestii płatności zbliżeniowych.

Ad 1

Zgodnie z art. 2 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2012 r. poz. 1149 j.t. z późn. zm.) „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, przez realizację celów określonych, w szczególności w ustawie z dnia 29 sierpnia 1997 r. - Prawo bankowe, ustawie z dnia 22 maja 2003 r. o nadzorze ubezpieczeniowym i emerytalnym oraz Rzeczniku Ubezpieczonych, ustawie z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym, ustawie z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych, ustawie z dnia 15 kwietnia 2005 r. o nadzorze uzupełniającym nad instytucjami kredytowymi, zakładami ubezpieczeń, zakładami reasekuracji i firmami inwestycyjnymi wchodzącymi w skład konglomeratu finansowego oraz ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych.”.

Mając na uwadze kwestie dotyczące ochrony danych osobowych należy stwierdzić, że kompetencje organu nadzoru w tym przedmiocie ograniczają się do badania zgodności działalności prowadzonej przez bank nie z przepisami ustawy z dnia 29 sierpnia 1997 r. o

ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 j.t. z późn. zm.) lecz ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376 j.t. z późn. zm.) w zakresie naruszania przepisów dotyczących ochrony tajemnicy bankowej, względnie do kontroli systemu zarządzania ryzykiem, szczególnie operacyjnym. Warto w tym miejscu podkreślić, że do Urzędu KNF nie napływały dotąd sygnały odnoszące się do kwestii bezpieczeństwa danych osobowych w związku z korzystaniem przez klientów z kart płatniczych wyposażonych w moduły płatności zbliżeniowych.

Ad 2

Pojęcie płatności zbliżeniowych nie jest pojęciem prawnym, określa ono tylko sposób zainicjowania transakcji płatniczej w tzw. „komunikacji bliskiego zasięgu” (ang. NFC – „Near Field Communication”). Zarówno dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE, 2006/48/WE i uchylająca dyrektywę 97/5/WE (Dz. U. UE L 319 z 5.12.2007 r., str. 1), jak i implementująca ją ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2011 r., Nr 199, poz. 1175, dalej: „UUP”) nie posługują się pojęciem płatności zbliżeniowych. Nie oznacza to jednak, że tego rodzaju płatności nie są objęte zakresem stosowania UUP.

Płatności zbliżeniowe będące przedmiotem wystąpienia należy zaliczyć do kategorii usług płatniczych objętych UUP. W tym przypadku karta płatnicza wydana przez bank (wyposażona w technologię NFC) jest instrumentem płatniczym, zdefiniowanym w art. 2 pkt 10 UUP wykorzystywanym przez użytkownika do złożenia zlecenia płatniczego w rozumieniu art. 2 pkt 36 UUP. Użycie karty wyposażonej w technologię NFC inicjuje transakcję płatniczą, o której mowa w art. 2 pkt 29 UUP.

Stosowanie UUP do płatności zbliżeniowych oznacza konieczność przestrzegania wzajemnych praw i obowiązków przez bank jako dostawcę usługi płatniczej i jego klienta jako użytkownika takiej usługi.

Zgodnie z art. 27 pkt 2 UUP dostawca usług płatniczych (bank) przekazuje użytkownikowi informacje dotyczące korzystania z usługi płatniczej obejmujące m.in.: (a) opis najważniejszych cech świadczonej usługi płatniczej, (b) wyszczególnienie informacji, które muszą być dostarczone przez użytkownika, aby zlecenie płatnicze mogło zostać prawidłowo wykonane albo informację, że wystarczające jest podanie unikatowego identyfikatora w rozumieniu art. 2 pkt 33 UUP), (c) określenie sposobu i procedury udzielania zgody na wykonanie transakcji płatniczej oraz wycofywania takiej zgody.

Na podstawie art. 40 ust. 1 UUP transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na jej wykonanie w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zatem umowa powinna określać w sposób szczegółowy sposób autoryzacji transakcji płatniczej przy użyciu indywidualnych zabezpieczeń tego instrumentu (np. kod PIN). Jest to szczególnie ważne dla dostawcy (banku) albowiem na nim spoczywa ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo (art. 45 ust. 1 UUP). Należy też mieć na uwadze, że wykazanie przez

dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 UUP. Brak zatem konieczności stosowania indywidualnych zabezpieczeń przez użytkownika skutkować może ponoszeniem odpowiedzialności za nieautoryzowane transakcje płatnicze przez dostawcę (bank).

W przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca usług płatniczych płatnika jest obowiązany (art. 45 UUP) niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. Jednakże płatnik odpowiada za nieautoryzowane transakcje płatnicze do wysokości równowartości w walucie polskiej 150 euro, ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji, jeżeli nieautoryzowana transakcja jest skutkiem posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub przywłaszczenia instrumentu płatniczego lub jego nieuprawnionego użycia w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2 UUP. Ponadto płatnik odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 UUP.

Ustalając zakres wzajemnych praw i obowiązków pomiędzy posiadaczem instrumentu płatniczego oraz dostawcą wydającym ten instrument niezwykle istotne jest określenie, czy instrument płatności zbliżeniowej podlega ograniczeniom, o których mowa w art. 39 UUP, czy też nie. Artykuł 39 ust. 1 UUP stanowi, że w przypadku instrumentów płatniczych, które zgodnie z umową ramową pozwalają na dokonywanie indywidualnych transakcji płatniczych na kwotę nieprzekraczającą równowartości w walucie polskiej 30 euro albo które mają limit wydatków w wysokości równowartości w walucie polskiej 150 euro, albo służą do przechowywania środków pieniężnych w kwocie nieprzekraczającej w żadnym momencie równowartości w walucie polskiej 150 euro¹, ustalonych przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu zawarcia umowy, dostawca i użytkownik mogą uzgodnić, że niektóre z obowiązków nałożonych na strony nie będą musiały mieć zastosowania. Zatem powyższe kryterium ilościowe determinuje czy dana karta zbliżeniowa spełnia wymogi przewidziane dla mikropłatności, czy też nie i czy w związku z tym strony mogą odstąpić od konieczności stosowania niektórych z określonych w UUP obowiązków.

¹ W przypadku transakcji płatniczych wykonywanych w całości na terytorium Rzeczypospolitej Polskiej ww. kwoty mogą zostać w umowie ramowej podwyższone o 100%. Natomiast w odniesieniu do przedpłaconych instrumentów płatniczych w zakresie transakcji płatniczych wykonywanych w całości na terytorium Rzeczypospolitej Polskiej określone w ust. 1 kwoty wynoszą równowartość w walucie polskiej 500 euro, ustaloną z zastosowaniem kursu średniego ogłaszanego przez NBP obowiązującego w dniu zawarcia umowy.

W przypadku spełniania kryterium przewidzianego przez art. 39 ust. 1 UUP (np. karta płatnicza z limitem na pojedyncze transakcje płatnicze do równowartości w walucie polskiej 60 euro) strony umowy o instrument płatniczy mogą uzgodnić m.in., że:

(1) jeżeli instrument płatniczy nie pozwala na jego zablokowanie lub uniemożliwienie w inny sposób jego dalszego używania, to wówczas nie stosuje się przepisów art. 42 ust. 1 pkt 2, art. 43 ust. 1 pkt 3-5 i art. 46 ust. 4 i 5 UUP.

Oznaczać to może w praktyce m.in., że (a) użytkownik uprawniony do korzystania z karty zbliżeniowej nie musi być zobowiązany do zgłaszania niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu, (b) dostawca wydający instrument płatniczy nie musi być zobowiązany do zapewnienia stałej dostępności odpowiednich środków pozwalających użytkownikowi na dokonanie zgłoszenia o utracie, kradzieży, przywłaszczeniu albo nieuprawnionym użyciu instrumentu płatniczego lub nieuprawnionym dostępie do tego instrumentu, (c) dostawca wydający instrument płatniczy nie musi być zobowiązany do zapewnienia procedur pozwalających na udowodnienie dokonania zgłoszenia, o którym mowa powyżej, (d) dostawca wydający instrument płatniczy nie musi być zobowiązany do uniemożliwienia korzystania z instrumentu płatniczego po dokonaniu zgłoszenia, (e) płatnik może nadal odpowiadać za nieautoryzowane transakcje płatnicze, nawet po dokonaniu stosownego zgłoszenia dostawcy i nawet gdy dostawca nie zapewnia odpowiednich środków umożliwiających dokonanie w każdym czasie takiego zgłoszenia;

(2) jeżeli instrument płatniczy jest używany anonimowo lub dostawca z innych przyczyn nieodłącznie związanych z instrumentem płatniczym nie jest w stanie udowodnić, że transakcja była autoryzowana, to wówczas nie stosuje się przepisów art. 45 oraz art. 46 ust. 1-3 UUP.

Może to wskazywać w praktyce m.in., że (a) ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, nie musi już spoczywać na dostawcy tego użytkownika, (b) wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego może być wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana, (c) dostawca nie musi być obowiązany udowodnić innych okoliczności wskazujących na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujących, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia obowiązku podjęcia niezbędnych środków służących zapobieżeniu naruszeniu indywidualnych zabezpieczeń tego instrumentu, w szczególności do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz do nieudostępniania go osobom nieuprawnionym, (d) w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika nie musi być obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja

płatnicza, (e) płatnik może odpowiadać za nieautoryzowane transakcje płatnicze w pełnej wysokości do czasu zgłoszenia zgodnie z art. 42 ust. 1 pkt 2 UUP, chyba że po dokonaniu zgłoszenia płatnik doprowadził umyślnie do nieautoryzowanej transakcji.

Zatem kwalifikacja płatności zbliżeniowych jako mikropłatności na podstawie art. 39 UUP pozwala pod pewnymi warunkami dostawcy usług płatniczych na rezygnację z niektórych obowiązków względem użytkownika karty z funkcją NFC w szczególności w sytuacjach niewykonania lub niewłaściwego wykonania usługi płatniczej. Warto mieć też na uwadze, że określenie sposobu autoryzacji transakcji płatniczej i określanie indywidualnych zabezpieczeń instrumentu płatniczego nie zostały szczegółowo uregulowane w UUP. Artykuł 26 w związku z art. 27 UUP stanowi jedynie, że umowa ramowa pomiędzy dostawcą a użytkownikiem usługi płatniczej powinna określać sposób i procedurę udzielania zgody na wykonanie transakcji płatniczej oraz wycofywania takiej zgody. Zagadnienie to zostało również w sposób ogólny przedstawione w art. 40 UUP, na podstawie którego transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na jej wykonanie w sposób przewidziany w umowie między płatnikiem a jego dostawcą.

Mając powyższe na uwadze niezwykle istotną jest kwestia pozostawienia pełnego i świadomego wyboru użytkownikowi w podejmowaniu decyzji, co do zamiaru korzystania z karty płatniczej kwalifikowanej do dokonywania mikropłatności w formule objętej przepisem art. 39 UUP, jak i wyboru korzystania z funkcji zbliżeniowej w przypadku otrzymania instrumentu płatniczego wyposażonego w ten moduł płatności.

Do tematyki kart zbliżeniowych zastosowanie mają również zalecenia wydanej przez KNF w styczniu 2013 r. Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach - stanowiącej załącznik do uchwały Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. (Dz. Urz. KNF z 2013 r. poz. 5) - dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, w szczególności dotyczące potrzeby stosowania możliwie niezawodnych metod i środków potwierdzania tożsamości i uprawnień klientów korzystających z elektronicznych kanałów dostępu. Należy jednak zwrócić uwagę, że znowelizowana Rekomendacja D powinna zostać wprowadzona w bankach do dnia 31 grudnia 2014 r. Stosunkowo długi czas na wprowadzenie Rekomendacji wynika m.in. ze znacznego zakresu zmian w stosunku do wersji Rekomendacji D wydanej w grudniu 2002 r. oraz konieczności przeprowadzenia przez banki rzetelnych, kompleksowych analiz przed przystąpieniem do wdrażania znowelizowanej Rekomendacji. Szacuje się, że pełen proces przeprowadzenia takiej analizy w przypadku średnich i dużych banków może trwać od 3 do 6 miesięcy.

W świetle Rekomendacji D (z roku 2002) i identyfikowanych zagrożeń dotyczących płatności zbliżeniowych można byłoby uznać za częściowo uzasadnione stwierdzenie, że systemy bankowości elektronicznej w tym zakresie mogą nie być jeszcze w pełni zgodne z zaleceniami opisanymi w sekcji „Szczególne mechanizmy kontroli bezpieczeństwa dotyczące bankowości elektronicznej”, w szczególności że mogą one nie być „zaprojektowane w sposób zmniejszający prawdopodobieństwo zainicjowania przez upoważnionych użytkowników

niezamierzonych transakcji” i że nie jest pewne, czy banki będą stosować w tym zakresie „niezawodne metody potwierdzenia tożsamości i uprawnień aktualnych klientów dążących do zainicjowania transakcji elektronicznych”. Obszar ten będzie dopiero przedmiotem badań w ramach działań nadzorczych KNF. Należy pamiętać, że Rekomendacja D w wersji przyjętej przez organ nadzoru w 2002 roku koncentrowała się zasadniczo na systemach bankowości elektronicznej albowiem ta forma zlecania transakcji płatniczych drogą elektroniczną była wówczas najbardziej rozpowszechniona, natomiast płatności zbliżeniowe pojawiły się kilka lat później.

Warto w tym miejscu wskazać także na charakter prawny rekomendacji wydawanych przez KNF. Rekomendacje KNF nie stanowią źródła prawa w Polsce, mają one charakter generalny i abstrakcyjny, są jedynie wskazaniem przez organ nadzoru pożądanego sposobu prowadzenia przez bank działalności, w tych przypadkach, gdy przepisy prawa nie regulują tego lub czynią to w sposób niedookreślony, a istnieją przesłanki dla ukształtowania dobrej praktyki rynkowej w danym obszarze. Podkreślić należy też, iż rekomendacje umożliwiają organowi nadzoru tylko i wyłącznie niewładcze oddziaływanie na podmioty nadzorowane, poprzez wskazywanie pożądanego sposobu prowadzenia przez bank działalności oraz mają na celu ukształtowanie dobrej praktyki rynkowej w danym obszarze. Dokument o charakterze niewładczym nie może upoważniać organu nadzoru do zobowiązywania podmiotów nadzorowanych do określonego działania bądź zaniechania. Moc zobowiązująca, czy też sankcjonująca przepisu może wynikać z jednego ze źródeł prawa powszechnie obowiązującego. Obowiązek ostrożnego i stabilnego zarządzania bankiem wynika wprost z ustawy - Prawo bankowe i nieprzestrzeganie tego wymogu daje możliwość zastosowania przez organ nadzoru sankcji wobec podmiotu nadzorowanego. Nie można jednak z tego wnioskować o mocy powszechnie obowiązującej dokumentu jakim jest rekomendacja Komisji Nadzoru Finansowego.

Ad 3

Do Urzędu KNF napływają różnego rodzaju sygnały, dotyczące bezpieczeństwa transakcji płatniczych, dokonywanych za pomocą kart płatniczych wyposażonych w moduły płatności zbliżeniowych. Urząd KNF zidentyfikował zagrożenia dotyczące m.in.:

- 1) możliwości dokonania transakcji zbliżeniowych na łączną kwotę lub w liczbie przekraczającej zadeklarowany przez klienta limit,
- 2) możliwości wykorzystania urządzeń pośredniczących w celu przeprowadzenia transakcji zdalnie obciążającej cudzą kartę zbliżeniową,
- 3) możliwości nieuprawnionego odczytania danych osobowych, numeru karty i innych informacji z karty zbliżeniowej,
- 4) możliwości częściowego sklonowania karty zbliżeniowej.

Należy także wskazać, że w grudniu 2012 r. KNF opublikowała w swoim serwisie internetowym dokument „Mobilne płatności zbliżeniowe – o czym warto wiedzieć?”, w którym zwrócono uwagę na ryzyko charakterystyczne dla tego rodzaju płatności oraz na potrzebę stosowania przez użytkowników tej technologii podstawowych zasad

bezpieczeństwa. KNF objęła również patronatem konferencję pt. „Warsztaty dla Sędziów, Prokuratorów oraz przedstawicieli KNF, GIIF i Policji nt. przeciwdziałania wykorzystywaniu bankowości elektronicznej do popełniania przestępstw”, na których przedstawiana była m.in. problematyka kart zbliżeniowych. W dniu 13 marca 2013 r. wystosowano wezwanie do wybranej grupy banków, celem pozyskania wyjaśnień w kwestii oferowania tego typu kart płatniczych i zagrożeń z tym związanych. Trwają obecnie w Urzędzie KNF analizy przesyłanych odpowiedzi.

Problematyka kart zbliżeniowych była także poruszona na posiedzeniu Rady ds. Systemu Płatniczego przy NBP w dniu 21 marca 2013 r. Ustalono, że eksperci Związku Banków Polskich przygotowują opracowanie dotyczące oceny poziomu bezpieczeństwa kart zbliżeniowych z punktu widzenia ich posiadaczy – planuje się przedstawienie tego opracowania na posiedzeniu Rady ds. Systemu Płatniczego w czerwcu 2013 r. Niezależnie od powyższego, materiał w przedmiotowym zakresie zostanie opracowany i przedstawiony na posiedzeniu ww. Rady również przez Urząd KNF. Zgodnie z aktualnie przyjętymi założeniami, w celu przeprowadzenia powyższej analizy Urząd KNF podejmie działania mające na celu pozyskanie wiedzy dotyczącej technicznych aspektów funkcjonowania instrumentów płatności zbliżeniowych, w tym m.in.:

- 1) wykorzystywanych przez banki mechanizmów kontrolnych w przedmiotowym zakresie, w tym korzystania z limitów off-line oraz możliwości uzyskania przez klienta karty nieposiadającej funkcji płatności zbliżeniowych bądź z opcją wyłączenia tej funkcji,
- 2) sposobu i zakresu analiz ryzyka, przeprowadzonych przez banki w związku z wdrożeniem produktów wykorzystujących technologię zbliżeniową, zidentyfikowanego ryzyka w tym zakresie i sposobów jego monitorowania,
- 3) specyfikacji technicznej kart zbliżeniowych, w szczególności zakresu danych możliwych do odczytania bez konieczności ich deszyfrowania oraz minimalnej odległości, przy której możliwa jest komunikacja z kartą bez konieczności stosowania urządzeń o znacznej wielkości.

W ramach analizy przeprowadzonej przez Urząd KNF wykorzystanie zostanie również dokument „Privacy and Data Protection Impact Assessment Framework for RFID Applications”, w szczególności załączniki II-IV. Wyniki powyższych analiz zostaną uwzględnione przy podejmowaniu decyzji dotyczących dalszych działań regulacyjno-nadzorczych.

Do Urzędu KNF docierają również sygnały o stosowaniu przez niektóre banki praktyki polegającej na braku możliwości wyboru przez klienta banku karty płatniczej innego rodzaju niż karty wyposażone w funkcję zbliżeniową. O ile wydanie użytkownikowi karty płatniczej wyposażonej automatycznie w funkcję zbliżeniową, która może być dodatkowo aktywowana tylko i wyłącznie na wyraźne życzenie użytkownika nie jest kwestią problematyczną, o tyle brak pozostawienia klientowi swobodnego i pełnego wyboru w zakresie korzystania z funkcji zbliżeniowej w karcie wymaga przeprowadzenia pogłębionych analiz prawnych mających na celu wyeliminowanie ryzyka stosowania przez banki niedozwolonych praktyk rynkowych w tym zakresie.

Dodatkowo należy wskazać, że w trakcie prac nad nowelizacją UUP (w zakresie proponowanego nowego art. 32a UUP) Urząd KNF postulował, aby obowiązek wskazania użytkownika karty płatniczej w umowie obejmował swym zakresem nie tylko umowy ramowe, ale również umowy o pojedyncze transakcje płatnicze. Propozycja Urzędu KNF miała na celu uniknięcie sytuacji, w której wydawca kart płatniczych wydawanych tylko do dokonania pojedynczej transakcji płatniczej nie będzie zobowiązany do identyfikowania użytkownika takiej karty. Potencjalnie prowadzić to może do nadużyć ze strony wydawców w szczególności w kontekście stosowania przepisów ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Dodatkowo w przypadku wydawców będących bankami, proponowane rozwiązania rodzą wątpliwości co do ich zgodności z przepisem artykułu 65 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, zgodnie z którym bank dokonujący wypłat z rachunku bankowego jest obowiązany sprawdzić autentyczność i prawidłowość formalną dokumentu stanowiącego podstawę do wypłaty oraz tożsamość osoby dającej zlecenie.

Podsumowując należy stwierdzić, że w kontekście problematyki kart zbliżeniowych wydawanych przez banki, w zakresie właściwości organu nadzoru ochrona danych osobowych użytkowników kart zbliżeniowych zasadniczo sprowadza się do weryfikowania zgodności działalności banków z przepisami ustawy - Prawo bankowe w kontekście naruszania przepisów dotyczących ochrony tajemnicy bankowej i do kontroli systemu zarządzania ryzykiem.

Przepisy UUP przewidują możliwość modyfikowania praw i obowiązków między bankiem, a jego klientem w przypadku dokonywania tzw. mikropłatności (które są popularne w przypadku płatności kartami zbliżeniowymi) – w kierunku mniejszej ochrony klienta banku (możliwość umownego ograniczenia stosowania określonych prokonsumenckich przepisów UUP wskazanych w pkt 2 niniejszego pisma).

Do Urzędu KNF nie napływały dotąd sygnały odnoszące się do kwestii bezpieczeństwa danych osobowych w związku z korzystaniem przez klientów z kart płatniczych wyposażonych w moduły płatności zbliżeniowych, jednakże wzrost popularności tego rodzaju produktu bankowego, generować może wzrost ryzyka nie tylko w tym obszarze, ale również w zakresie bezpieczeństwa transakcji płatniczych. Kwestie te będą podlegały monitoringowi Urzędu KNF w celu ewentualnego podjęcia stosownych działań regulacyjno-nadzorczych.

Odrębnym przedmiotem analiz winna być kwestia pozostawienia klientowi swobodnego i pełnego wyboru w zakresie korzystania z funkcji zbliżeniowej w wydanej mu karcie płatniczej w kontekście stosowania przez banki niedozwolonych praktyk rynkowych w tym zakresie. Na obecnym etapie za pożądany kierunek należałoby uznać przyjęcie przez dostawców usług płatniczych praktyki polegającej na pozostawieniu użytkownikowi instrumentu płatniczego wyposażonego w funkcję zbliżeniową daleko idącej swobody w samodzielnym lub uzgodnionym z dostawcą wymogu autoryzacji transakcji zbliżeniowej za pomocą indywidualnych zabezpieczeń tego instrumentu w postaci kodu PIN.