EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Odpowiedzi Europejskiego Kongresu Finansowego[1] w konsultacjach Europejskiego Urzędu Nadzoru Bankowego dotyczących FinTech[2]

Metodologia opracowania odpowiedzi

Opracowanie stanowiska przebiegało w następujących etapach:

Etap 1

Do wzięcia udziału w badaniu zaproszono liczną grupę ekspertów z polskiego sektora finansowego, do których przesłano wybrane fragmenty dokumentu konsultacyjnego EBA oraz pytania konsultacyjne w języku polskim.
Ekspertom zagwarantowana została anonimowość.

Etap 2

Na bazie uzyskanych opinii opracowana została propozycja syntezy odpowiedzi. Odpowiedzi uzyskano od ekspertów reprezentujących:

- banki,
- firmy FinTech,
- firmy ubezpieczeniowe,
- instytucje regulacyjne,
- firmy konsultingowe i kancelarie prawne,
- środowisko naukowe.

Propozycję tę przekazano ekspertom, którzy wzięli udział w konsultacjach. Zwrócono się do nich z prośbą o zaznaczenie w syntezie tych sformułowań, które powinny zostać zmodyfikowane i zaproponowanie modyfikacji czy dodatkowych zapisów, jak również zaznaczenie tych opinii, z którymi się nie zgadzają i które powinny być z ostatecznej syntezy usunięte.

Etap 3

Po uwzględnieniu uwag ekspertów opracowane zostały ostateczne syntetyczne odpowiedzi Europejskiego Kongresu Finansowego przedstawione poniżej.

---

[1] Celem Europejskiego Kongresu Finansowego (www.efcongress.com) jest debata nt. bezpieczeństwa i rozwoju sektora finansowego Unii Europejskiej i Polski.

[2] http://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf

Odpowiedzi Europejskiego Kongresu Finansowego

1. Czy kwestie określone przez EBA i dalsze kroki proponowane w sekcji 4.1 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Większość zapisów dobrze oddaje sytuację. Trafnym spostrzeżeniem jest brak regulacji i nadzoru dla znacznego zakresu instytucji, w tym określanych jako fintech i działających w obszarze finansów.

Nadzór i regulacje powinny obejmować poszczególne podmioty zależnie od realnie wykonywanych przez nie działań, ich charakteru i skali, a nie formalnego sposobu funkcjonowania na rynku. Status „fintech" nie powinien być powodem dla lepszego traktowania. Na rynkach konkurencyjnych, o wysokim poziomie innowacyjności, takich jak Polska, nie ma powodów dla preferencyjnego traktowania wybranych podmiotów ze względu na ich charakter.

Rozwiązania typu sandbox i ułatwienia, o ile się pojawią, powinny dotyczyć każdego podmiotu, także banku a nie tylko fintech, o ile rozwiązania testowane w sandbox spełnią jednolite kryteria (wartości, wolumeny etc.). Oczywiście w praktyce dotyczyłyby startupów o charakterze fintechów.

Kluczowe dla nadzorów powinno być zachowanie bezpieczeństwa systemowego i bezpieczeństwa klientów, bez względu na rodzaj podmiotu świadczącego usługi o charakterze finansowym/bankowym dla klientów.

W zakresie innowacyjności korzystne może być pozostawienie swobody na poziomie krajowym, a następnie wymiana wiedzy i wdrażanie najlepszych praktyk na poziomie europejskim.

2. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.2.1 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Tak, są trafne i we właściwy sposób wskazują kierunek.

Wartym wskazania elementem uzupełniającym do proponowanych przez EBA dalszych kroków, wydaje się być zacieśnienie współpracy i wymiany wiedzy pomiędzy organami nadzoru w krajach członkowskich.

W zakresie cyberbezpieczeństwa warto zwrócić uwagę, że bezpieczeństwo jest takie jak jego najsłabszy element. Szerokie dopuszczenie podmiotów mniej regulowanych do systemów bankowych - o czym jest mowa np. w PSD2 (usługi PIS i AIS) - niesie istotne ryzyko systemowe dla sektora bankowego, ponieważ bez umów bank nie będzie miał żadnego wpływu na sposób zarządzania danymi w gestii tzw. podmiotów trzecich (TPP), a braki w systemach fintech (mniej regulowanych lub poza regulacjami) mogą w praktyce wpłynąć na wypływanie środków i danych klientów bankowych. Tym samym widać zasadność objęcia TPP szerokim nadzorem. Wskazane tu ryzyko może być widoczne w dłuższej perspektywie. Wypływ danych bankowych z fintechów może negatywnie odbić się nie tylko na podmiotach fintech, ale także na sektorze bankowym i osłabić zaufanie do sektora bankowego.

3. Jakie szanse i zagrożenia wynikające z FinTech mogą powstać dla instytucji kredytowych?

Wybrane szanse:

- zwiększenie innowacyjności modeli biznesowych instytucji finansowych,
- dalsza digitalizacja modeli biznesowych,
- większa elastyczność,
- szersze analizy danych, informacji, możliwość budowania lepszych modeli scoringowych i oceny ryzyka,
- dalsza automatyzacja procesów służących obsłudze klientów, w tym ograniczenie kosztów i błędów ludzkich,
- obniżenie kosztów funkcjonowania instytucji finansowych,
- szybsza realizacja usług (szybsze podejmowanie decyzji, np. kredytowych),
- nowe modele biznesowe.

Zagrożenia:

- przy powierzchownym podejściu w praktyce mniej wiarygodny scoring finansowy (szybsze decyzje finansowe w oparciu o dane z zewnętrznych źródeł) w modelu fintech,
- naruszenie bezpieczeństwa, poufności i integralności danych,
- nierówna konkurencja: fintech jako podmioty nieregulowane lub mniej regulowane, a oferujące te same produkty co silnie regulowane banki, choć dzięki temu fintech mogą w krótkiej perspektywie mieć przewagę nad bankami, to w długiej perspektywie będą generowały znacznie większe niż banki ryzyko,
- rozluźnienie relacji banków z klientami i utrudnienie oferowania usług cross sell i pakietowych, a tym samym postawienie banków w dużo gorszej pozycji konkurencyjnej w stosunku do promowanych instytucji fintech,
- utrudnione sprawowanie nadzoru,
- ryzyka płynące z mniejszego rygoru bezpieczeństwa w podmiotach nieregulowanych,
- wzrost cyberzagrożeń (np. nowe modele przejęcia rachunków bankowych),
- pojawienie się nowych ryzyk związanych z nowymi modelami biznesowymi.

4. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.2.2 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

W usługach finansowych krytyczne jest zachowanie bezpieczeństwa systemowego i bezpieczeństwa klientów. Istotne jest znalezienie równowagi pomiędzy rozwojem innowacyjnych form płatności, a zachowaniem optymalnego poziomu bezpieczeństwa i zaufania do elektronicznych środków płatniczych. Banki powinny móc określać własną politykę w tym zakresie.

W zakresie DLT i Blockchain, EBA powinna zebrać analizy banków centralnych i sektora finansowego i bazować na nich w proponowanych analizach własnych i wynikających z nich rekomendacjach.

Ze względu na zróżnicowanie rynków w UE, opracowanie jednolitych wniosków może nie być możliwe i może nieść ryzyko dla niektórych rynków (szczególnie tych z efektywniejszym nadzorem).

5. Jakie szanse i zagrożenia wynikające z FinTech mogą powstać dla instytucji płatniczych i instytucji pieniądza elektronicznego?

Podobnie jak w pkt 3, w szczególności:

Szanse:

- efektywniejsze płatności transgraniczne (cross-border),
- łatwiejszy dostęp do usług i ich szybsza realizacja,
- dalszy rozwój płatności bezgotówkowych,
- niższe koszty transakcji transgranicznych,
- rozwiązania typu robo-advisory,
- nowe sposoby, w szczególności biometryczne, identyfikacji i autentykacji użytkownika w procesie uwierzytelniania, w tym na potrzeby płatności.

Zagrożenia:

- zwiększone ryzyko transakcji oszukańczych,
- ryzyko związane z AML (szczególnie w płatnościach cross-border oraz P2P),
- naruszenie bezpieczeństwa, poufności i integralności danych,
- naruszenie zasad uczciwej konkurencji poprzez promowanie lub ograniczanie wymogów dla podmiotów ze względu na ich status (fintech).

6. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.3.1 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Stanowisko nie wymaga dodatkowego komentarza. Podkreślenia może wymagać potrzeba dzielenia się wiedzą.

7. Jaki może być wpływ stosowania innowacji finansowych opartych na nowoczesnych technologiach i/lub wzrostu liczby firm świadczących usługi z obszaru FinTech oraz zwiększenia zakresu i skali ich działalności na model biznesowy istniejących instytucji kredytowych?

- dalsza cyfryzacja oraz automatyzacja,
- obniżenie kosztów,

- spadek marż (ryzyko systemowe dla podmiotów regulowanych ze względu na wysoki poziom kosztów „regulacyjnych”),
- poprawa jakości usług,
- ograniczenie dostępności nowych usług dla osób wykluczonych cyfrowo,
- większe ryzyko systemowe,
- mniejsze bezpieczeństwo klientów w rezultacie coraz powszechniejszego korzystania z nieregulowanych nowych podmiotów (w praktyce oferujących często niższy poziom bezpieczeństwa).

8. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.3.2 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Kwestie nie zostały jeszcze określone, więc trudno je oceniać.

Wywiady powinny być prowadzone z szerszym zakresem podmiotów, w szczególności z regulatorami, bankami, instytucjami płatniczymi oraz tzw. fintechami. W ramach rozmów warto uwzględnić także podmioty CERT.

9. Jaki może być wpływ stosowania innowacji finansowych opartych na nowoczesnych technologiach i/lub wzrostu liczby firm świadczących usługi z obszaru FinTech oraz zwiększenia zakresu i skali ich działalności na modele biznesowe istniejących instytucji zajmujących się płatnościami lub instytucji pieniądza elektronicznego?

- innowacje finansowe oparte na nowych technologiach powodują zmianę podejścia i ewolucję modeli biznesowych,
- przyśpieszenie ewolucji banków,
- większe ryzyko systemowe jako pochodna szybszych zmian,
- trudność w nadążaniu za zmianami przez regulatorów,
- zbytnia koncentracja na wygodzie kosztem bezpieczeństwa, co szczególnie w dłuższym okresie może być niebezpieczne (cyfrowe bezpieczeństwo będzie niewystarczające).

10. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.4.1 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Ochrona konsumenta jest kluczowa, niezależnie od tego jaki podmiot świadczy usługi finansowe czy płatnicze, a także z jakiego kraju pochodzi dostawca, jak również niezależnie od tego, jakie podmioty współpracują ze sobą w świadczeniu danej usługi (w tym jaka jest forma prawna tej współpracy). Duże znaczenie będzie miała współpraca między regulatorami.

11. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.4.2 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

EBA trafnie zauważa szczególny problem ochrony praw konsumentów w sytuacji świadczenia usług transgranicznych, szczególnie w kontekście ograniczonego poziomu harmonizacji przepisów prawa w państwach członkowskich i związanego z tym problemu arbitrażu regulacyjnego oraz obserwowanej praktyki przedsiębiorców polegającej na umownym wyłączaniu jurysdykcji sądów państwa stałego pobytu/zamieszkania konsumenta na rzecz sądów państwa siedziby przedsiębiorcy.

Duże znaczenie będzie miała współpraca między regulatorami.

12. Czy firmy FinTech napotkają przeszkody regulacyjne związane z ochroną konsumentów uniemożliwiające świadczenie transgraniczne usług finansowych?

Przeszkody regulacyjne w przypadku świadczenia transgranicznych usług finansowych, które mogą je potencjalnie uniemożliwić wydają się przede wszystkim wynikać z niejasności co do tego, które przepisy prawne, którego z państw, na których obszarze świadczone będą usługi, znajdą zastosowanie do ochrony konsumenta.

Brak spójnych regulacji w tym zakresie jest problemem nie tylko dla firm z branży fintech, ale dla wszystkich instytucji działających transgraniczne (w tym instytucji kredytowych, instytucji płatniczych i instytucji pieniądza elektronicznego) i wszelkie uproszczenia nie powinny koncentrować się na ułatwianiu prowadzenia działalności podmiotom fintech, ale na ułatwianiu działalności transgranicznej jako takiej.

Wchodzące regulacje RODO mogą ograniczyć ryzyko związane z ochroną danych osobowych.

W praktyce jednak patrząc na rozwój fintech nie wydaje się, żeby przeszkody regulacyjne związane z ochroną konsumentów w sposób nadmierny utrudniały czy wręcz uniemożliwiały świadczenie transgraniczne usług finansowych.

13. Czy EBA powinna podjąć dalsze działania w celu zapewnienia spójnego i konsekwentnego wdrażania w całej UE regulacji dotyczących usług finansowych?

Tak. Przy czym konieczne jest uwzględnianie specyfiki lokalnych rynków, umożliwienie innowacyjności nie tylko europejskiej ale i lokalnej oraz uwzględnianie elementów, które są lokalne i nie ma co do nich planów ujednolicenia (np. lokalne systemy gwarantowania depozytów).

Warto także dodać, że szczególnie banki już są przeregulowane i należy ostrożnie podchodzić do narzucenia nowych obowiązków, aby nie stanowiły one nieuzasadnionych obowiązków równoległych w stosunku do już istniejących. Ten problem nie dotyczy oczywiście podmiotów obecnie nieregulowanych.

14. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.4.3 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Na obecnym etapie rozwoju rynku fintech kwestie są trafne. Wątpliwości budzi brak odniesienia wprost do działań na styku bank – fintech, jeśli klient złoży reklamację do banku, który jest zobowiązany uznać dane roszczenie i dochodzić finansowania od podmiotów trzecich.

Warto aby ten obszar był przedmiotem regulacji nadzoru w celu uniknięcia regularnego kredytowania tego rodzaju roszczeń przez dostawców rachunków lub konieczności ponoszenia nieuzasadnionych kosztów na odzyskanie należności z tego tytułu.

15. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.4.4 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Kwestie są dobrze określone. Zasady transparentnego przekazywania informacji klientom powinny być jednakowe dla wszystkich dostawców usług bankowych/płatniczych, bez względu na formę działania.

16. Czy w przepisach krajowych jakiekolwiek wymogi dotyczące transparentności lub ujawniania informacji mogą stanowić poważne utrudnienie w procesach cyfryzacji lub uniemożliwić firmom FinTech wejście na rynek?

Nie ma przepisów, które dyskryminowałyby fintechy dlatego, że są fintechami.

Istnieje natomiast wiele przepisów wprowadzających rozliczne obowiązki, które stanowią naturalną barierę. Nie powinno się jednak oczekiwać, że fintechy zostaną z tych obowiązków zwolnione tylko dlatego, że są fintechami.

Należy jednak mieć na uwadze, że obecni gracze, a szczególnie banki muszą spełniać o wiele większe wymogi prawne, które, choć są elementem wpływającym istotnie na ich bezpieczeństwo, stawiają banki w gorszej pozycji konkurencyjnej względem nowych podmiotów. Także krajowe instytucje płatnicze już dziś muszą spełnić szereg wymogów, choć istotnie mniejszych niż banki.

17. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.4.5 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Kwestie zostały opisane trafnie, niemniej należy zauważyć, że o ile wiedza klientów o lokalnym prawie krajowym ma szanse być opisana i przedstawiona (co i tak nie jest proste, aby było przystępne), o tyle przy zawieraniu umów na odległość, w oparciu o prawo obce oraz kontrakty zawierane w innym języku, nie może być wystarczająca dla klientów.

Edukacja i pogłębianie wiedzy konsumentów to bez wątpienia warunek konieczny właściwego funkcjonowania każdego rynku. Należy mieć przy tym świadomość, że rozwój rynku postępuje obecnie w tempie nienotowanym nigdy w historii. Z tego

względu należy wdrażać najlepsze z punktu widzenia jak najbardziej aktualnego stanu wiedzy narzędzia edukacji konsumentów. Jak pokazuje jednak praktyka, nawet najlepsza edukacja może okazywać się niewystarczająca.

Ważne także, żeby edukacja nie dotyczyła tylko i wyłącznie sfery finansowej, ale również bezpieczeństwa, szczególnie cyberbezpieczeństwa.

18. Czy wskazane byłoby wprowadzenie specjalnych programów skierowanych do konsumentów w celu poprawy wiedzy o finansach oraz zwiększenia zaufania do usług cyfrowych?

Zdecydowanie tak, jest to warunek konieczny dla dalszego rozwoju usług cyfrowych. Wszelkie działania edukacyjne można postrzegać jako pożądane.

Ważne jest także, żeby edukacja nie dotyczyła tylko i wyłącznie sfery finansowej, ale również bezpieczeństwa, szczególnie cyberbezpieczeństwa.

Powstawanie nowych usług powinno wiązać się nie tylko z edukacją w zakresie korzyści z nowych usług (czyli w praktyce marketingu i promocji), ale także obejmować uczciwą edukację o ryzykach i sposobach przeciwdziałania (np. utrzymywania danych uwierzytelniających w poufności, aby faktycznie stanowiły element bezpieczeństwa który jest znany tylko użytkownikowi i jedynym innym podmiotem jaki może je zweryfikować był podmiot jaki je wydał).

Ważne jest również odpowiednie szkolenie pracowników sektora finansowego, którzy wchodzą w interakcje z klientami, tak aby sami mieli świadomość stosowanych w kanałach elektronicznych zabezpieczeń i potrafili wyjaśnić je klientom.

Przykładowo użycie API jako nowej metody dostępu do danych klienta otwiera cyberprzestępcom możliwość skorzystania z nowych wektorów ataku – zarówno na infrastrukturę jak i za pomocą social engineering. Przejęcie danych z banków mogłoby w konsekwencji doprowadzić do kradzieży nie tylko środków ale i tożsamości. Ze względu na wagę danych, które mogą zostać pozyskane, wyzwaniem jest właściwa edukacja klientów, aby zapobiegać potencjalnym nadużyciom w obszarze kanałów elektronicznego dostępu.

19. Czy kwestie określone przez EBA i dalsze kroki proponowane w podrozdziale 4.4.6 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

O ile kwestie są trafnie wskazane jako obszar, to należy zauważyć, że korzyści z takich metod jak analiza big data i AI wydają się przewyższać ich ewentualne negatywne efekty.

Problemem nie jest big data czy AI, a co najwyżej wykorzystanie konkretnych rodzajów danych. Sam proces gromadzenia i analizy danych niesie wiele korzyści i – przeciwnie do sugerowanej tezy – nie musi prowadzić do wykluczenia, ale może skutecznie umożliwić szerszy dostęp do usług, ponieważ pozwala zaoferować produkty niektórym odbiorcom, którym banki dotychczas usług nie proponowały. Umożliwienie bankom

korzystania z tych metod, z których fintechy już korzystają, może wyrównać szanse na dynamicznie rosnącym rynku.

Można zgłosić także kilka postulatów jako uzupełnienie, np.: kwestię wykorzystania AI w zakresie wirtualnych doradców typu chatbot w usługach bankowych (chatbot – głosowy i tekstowy, w tym w oparciu o komunikatory i media społecznościowe), a nie tylko robo-advisors rozumianych jako automatyczni doradcy finansowi (automation in financial advice/advisory).

W materiale nie wskazano także ryzyka związanego z koncentracją bardzo dużych i szerokich wolumenów danych populacji UE w „rękach" praktycznie kilku instytucji spoza UE, takich jak Facebook, Google, Amazon czy Apple.

20. Czy kwestie określone przez EBA i dalsze kroki proponowane w sekcji 4.5 są trafne i wyczerpujące? Jeśli nie, proszę wyjaśnić dlaczego.

Istnieje ryzyko nieuczciwej konkurencji ze strony szczególnie nieregulowanych podmiotów. W szczególności nie wszystkie fintechy podlegają PSD 2. Warto przeanalizować zależności i przemyśleć utworzenie scentralizowanego sposobu monitorowania nieuczciwych praktyk konkurencyjnych.

Zagadnienia opisane w sekcji 4.5 są szczególnie istotne ze względu na obecną i potencjalną skalę działania fintechów i możliwość ich wpływu nie tylko na europejski, ale także na globalny rynek finansowy. Przewaga konkurencyjna fintechów opiera się często na łatwości i szybkości obsługi, kosztem większego ryzyka, co jest pochodną braku nadzoru lub ograniczonego nadzoru.

O ile obserwacja rynku jest pierwszym krokiem, na pewno nie jest wystarczająca. W kolejnych krokach konieczne jest doprecyzowanie działań planowanych w tym obszarze.

21. Czy trafne jest określenie problemów wskazanych przez EBA i dalszych kroków proponowanych w sekcji 4.6? Czy są jakieś inne kwestie, które powinny być rozważone przez EBA?

Przedstawione kwestie oraz spostrzeżenia w sekcji 4.6, prezentowane są w sposób kompleksowy i spójny.

Warto rozważyć wymianę wiedzy z analogicznymi instytucjami także spoza Europy oraz szersze dzielenie się wiedzą przez nadzorców z uczestnikami rynku w celu doskonalenia metod w zakresie AML/CFT.

Słuszna jest uwaga, żeby wszystkie podmioty były jednolicie objęte regulacjami.

22. Jakie są największe ryzyka dotyczące prania pieniędzy i finansowania terroryzmu związane z firmami FinTech? Proszę wyjaśnić dlaczego.

- szybkość transferów pieniężnych, upowszechnianie płatności natychmiastowych,

- brak szerszego kontekstu transakcji, który pozwoliłby na zidentyfikowanie powiązań pomiędzy różnymi produktami, klientami – w klasycznym fintech jest widocznych mniej faktycznych przepływów i powiązań,
- brak zasobów i edukacji w fintech - niejednokrotnie są to startupy, w których świadomość ryzyk przychodzi na późniejszym etapie rozwoju,
- banki czy inne instytucje finansowe funkcjonują na rynku ściśle regulowanym, są instytucjami zaufania publicznego – natomiast fintechy to podmioty, których spektrum działalności nie jest uregulowane, problemy fintechów mogą negatywnie wpłynąć także na rynek bankowy,
- ryzyko dotyczące prania brudnych pieniędzy ma zarówno charakter inwestycyjny (nabywanie udziałów w firmach fintech, ryzyko baniek inwestycyjnych) jak i operacyjny – niekontrolowane przepływy finansowe mogące łatwiej pochodzić z nielegalnych źródeł,
- z usług fintech mogą korzystać organizacje przestępcze, operujące w sferze prania brudnych pieniędzy czy terroryzmu, które stać na nowoczesne rozwiązania informatyczne, które mogą pomóc im legitymizować ich przestępczą działalność, w tym także w oparciu o infrastrukturę bankową, fintechy nie mają tutaj wystarczających obowiązków informacyjnych – tak jak jest to w przypadku np. banków,
- automatyzacja i szybkość procesu onboardingu jaki stosuje większość fintechów immanentnie związana jest z większą nieprecyzyjnością procesu przeciwdziałania praniu pieniędzy, co zwiększa to ryzyko,
- łatwość anonimizacji stron transakcji sprzyja wykorzystaniu w działalności przestępczej.

23. Czy krajowe przepisy dotyczące zapobiegania praniu pieniędzy i finansowaniu terroryzmu stanowią przeszkody uniemożliwiające

(a) firmom FinTech wejście na rynek

Nie ma przepisów, które dyskryminowałyby fintechy dlatego, że są fintechami.

Warto zaznaczyć, że przepisy dotyczące zapobieganiu praniu brudnych pieniędzy i finansowaniu terroryzmu powinny przede wszystkim w sposób kompletny obejmować wszystkie podmioty, które prowadzą monitorowane transakcje, tak banki, fintechy jak i wszelkie inne podmioty. Każda firma dostarczająca produkty finansowe powinna zapobiegać praniu brudnych pieniędzy i finansowaniu terroryzmu.

(b) stosowanie rozwiązań FinTech przez zobowiązane podmioty w procesach due diligence? Proszę wyjaśnić.

Nie widać takich ograniczeń. Przy czym np. nie ma precyzyjnych zapisów stosowania np. identyfikacji biometrycznej przez podmioty obowiązane. Pewne rozwiązania techniczne stosowane w procesie DD mogą być wręcz pożądane (i już oferowane), jednak brak

regulacji w tym zakresie może zniechęcać do ich implementacji na szerszą skalę z uwagi na obawy o ewentualne zarzuty co do zasad i okoliczności ich stosowania.

Zastosowanie innowacji przez zobowiązane podmioty w procesach due diligence powinno być realizowane wyłącznie gdy ma pozytywny wpływ na ich efektywność oraz nie ma negatywnego wpływu na stabilność całego systemu.

24. Inne uwagi dotyczące opracowania EBA

Wszyscy znają możliwości jakie niosą fintechy i nowe rozwiązania. Bardzo cenne jest, że EBA spojrzała także na wiążące się z tym ryzyka. Takie podejście to także potencjalnie wyrównanie pozycji konkurencyjnej tradycyjnych graczy (głównie banki) oraz nowych podmiotów.

Warto zwrócić także uwagę na fakt, że po wejściu w życie PSD2 i RTS (SCA) banki będą ponosiły pełna odpowiedzialność za płatności zlecane z poziomu podmiotów trzecich – dlatego bardzo ważne jest, aby monitorować ryzyko całościowo i per podmiot. Ponieważ podmioty trzecie otrzymają możliwość łatwego dostępu do danych o rachunkach płatniczych klientów i możliwość zlecenia płatności, powinny przywiązywać bardzo dużą uwagę do ochrony danych klientów. Także w tym obszarze widać korzyści z inicjatywy EBA.

Na koniec należy wskazać także na następujące ogólne elementy:

- Niezbędna jest edukacja wszystkich stron: nadzorców, regulatorów, dostawców usług (tak banków jak i fintech) jak i klientów, aby działać możliwie bezpiecznie.
- Konieczne jest dzielenie się wiedzą między nadzorami oraz współpraca nadzorów z rynkiem.
- Dogmat wygody nie powinien przesłonić kwestii bezpieczeństwa, która w sektorze finansowym jest nadrzędna i w praktyce stanowi powód istnienia nadzorów.
- Poziom nadzoru i regulacji powinien być adekwatny do prowadzonej działalności i jej skali, niesionych ryzyk systemowych i ryzyk dla klientów, a nie tylko formy działania.