- **Czy zgadzacie się z argumentacją EBA uzasadniającą wymaganie silnego uwierzytelnienia klienta i zaproponowaną w Rozdziale 1 propozycji regulacyjnych standardów technicznych?**

Nie zgadzamy się ze stanowiskiem EBA wyrażonym w punkcie 19b rozdziału "Tło i uzasadnienie". Zgodnie z interpretacją EBA artykuł 74(2) PSD2 umożliwia odbiorcy lub jego dostawcy usług płatniczych zastosowanie opcji nieuznania silnego uwierzytelnienia klienta podczas krótkiego okresu przejściowego pomiędzy datą wdrożenia PDS2 (13 stycznia 2018) i datą wdrożenia regulacyjnych standardów technicznych (najwcześniej w październiku 2018). W naszej ocenie taka interpretacja nie jest uzasadniona przepisami PSD2. Uważamy, że nie ma podstaw prawnych ani przesłanek aby przyjąć taką interpretację. Analiza art. 98 PSD2 w naszej ocenie prowadzi do zupełnie odwrotnych wniosków niż te, które wskazuje EBA, szersza argumentacja dotycząca tego zagadnienia przedstawiona jest w odpowiedzi do pytania 4tego. Chcielibyśmy jednak zaznaczyć, iż funkcjonująca min. w zasadach organizacji kartowych zasada „liability shift" jest bezapelacyjnie jednym z najbardziej efektywnych środków ochrony użytkownika przed ewentualnymi stratami. Zasada liability shift działa z korzyścią zarówno dla akceptantów jak i płacących. Dzięki niej akceptanci mogą oferować lepsze i bardziej wygodne rozwiązania, np. płatności one-click, zwiększając konwersje i upowszechniając tym samym płatności bezgotówkowe. Nie ulega wątpliwości, że użytkownicy wybierają te rozwiązania, które w największym stopniu zapewniają szybki i wygodny transfer środków do odbiorcy. Wymuszanie silnego uwierzytelnienia dla każdej transakcji może z powodować i w naszej ocenie spowoduje odwrót użytkowników od płatności bezgotówkowych i powrót do płatności przy odbiorze (Cash On Delievery), co stoi w sprzeczności z podejmowanymi w ramach Unie Europaejskiej działaniami na rzecz rozwoju płatności bezgotówkowych.

Obserwowany obecnie dynamiczny rozwój płatności w środowisku internetowym, możliwy jest dzięki temu, iż akceptanci i dostawcy usług płatniczych mogą stosować podejście oparte o analizę ryzyka (risk based approach – RBA), które bardzo często daje ten sam, a często nawet wyższy poziom bezpieczeństwa jak w przypadku zastosowania „tradycyjnego" silnego uwierzytelnienie klienta. Nadmierne wywoływanie silnego uwierzytelniania klienta spowoduje obniżenie jego czujności, np. w przypadku popularnych w ostatnim czasie One-time passwords (OTPs) w formie sms-ów z kodem - klient po kilkudziesięciu, kilkunastu wywołaniach silnego uwierzytelnia w tym trybie nie będzie przykładał uwagi do treści SMS-a (np. kwoty czy odbiorcy) tylko bezrefleksyjnie przepisze kod co w kontekście wirusów umożliwiających modyfikowanie treści wiadomości SMS znacznie zwiększa ryzyko po stronie użytkownika (dotyczy to zwłaszcza starszych urządzeń nie wspieranych przez producentów oprogramowania, ale które wciąż w ogromnej ilości znajdują się na rynku). W tym miejscu warto również zauważyć, iż nowa wersja projektu Wytycznych w sprawie cyfrowej autentykacji (Digital Authentication Guideline) wydawanych przez Narodowy Instytut Stanów Zjednoczonych ds. Standaryzacji i Technologii (NIST) zniechęca przedsiębiorstwa do korzystania z uwierzytelniania opartego

na SMS dla celów dwuskładnikowego uwierzytelniania. W naszej ocenie podejście EBA powinno być bardziej nakierowane na kwestie ryzyka i praktyczne aspekty procesowanie transakcji zamiast na konkretne wąsko określone reguły. Rekomendujemy dopuszczenie możliwości niestosowania silnego uwierzytelnienia klientów w sytuacji gdy zasada „liability shift" jest uzgodniona pomiędzy dostawcami usług płatniczych prowadzącymi rachunek płacącego, a dostawcą usług płatniczych odbiorcy, jak ma to miejsce w przypadku schematów kartowych (gdy organizacje kartowe są odpowiedzialne za ustanawianie reguł) lub bilateralnych umów pomiędzy wydawcami instrumentów płatniczych, a agentami rozliczeniowymi. Schematy kartowe regulują min. maksymalne poziomy fraudów zarówno po stronie merchanta jak i acquirer'a co może być sugestią dla EBA, że wraz umożliwieniem RBA w szerokim zakresie warto rozważyć jednoczesne ustalenie maksymalnych poziomów fraudów.

- **Czy zgadzacie się z argumentacją EBA dotyczącą włączeń od stosowania art 97 dotyczącego silnego uwierzytelnienia klienta i środków bezpieczeństwa i propozycjami zawartymi w Rozdziale 2 propozycji regulacyjnych standardów technicznych?**

Nie zgadzamy się ze stanowiskiem EBA dotyczącym zagadnienia „risk based approach" wyrażonym w punkcie 3.2.2. Zgodnie z artykułem 98 PSD2 EBA „w ścisłej współpracy z EBC i po przeprowadzeniu konsultacji z wszystkimi stosownymi zainteresowanymi podmiotami, w tym podmiotami na rynku usług płatniczych, biorąc pod uwagę wszystkie stosowne interesy, opracowuje projekt regulacyjnych standardów technicznych (…) określających: b) wyłączenia ze stosowania art. 97 ust. 1, 2 i 3, na podstawie kryteriów ustanowionych w ust. 3 niniejszego artykułu". Jednocześnie paragraf 3 odnosi się wprost i bezpośrednio do poziomu ryzyka związanego ze świadczoną usługą.

„3. Wyłączenia, o których mowa w ust. 1 lit. b), są oparte na następujących kryteriach:
a) poziom ryzyka związanego ze świadczoną usługą;
b) kwota lub powtarzalny charakter transakcji lub oba te elementy;
c) kanał płatności używany do wykonania transakcji."

Pomimo jasnego wskazania RBA w tekście PSD2, EBA postanowiła nie wspominać zasady "risk based approach" w regulacyjnych standardach technicznych. W obecnym porządku prawnym (zwłaszcza w wydanych przez EBA *Rekomendacjach dotyczących bezpieczeństwa płatności internetowych*) zastosowanie silnego uwierzytelnienia klienta, w wielu przypadkach, pozostawione jest decyzji dostawcy usług płatniczych (w tym dostawcy usług płatniczych prowadzącego rachunek płatniczy), np. przelewy w ramach tego samego dostawcy usług płatniczych lub płatności kartowych. Dodatkowo uważamy, że mechanizm „risk based approach" powinien być wprowadzany we wszystkich metodach płatności, a nie tylko w odniesieniu do płatności kartowych i przelewów w ramach tego samego dostawcy usług płatniczych.

W naszej opinii mechanizm silnego uwierzytelnienia klienta powinien oparty o „risk

based approach" dla wszystkich transakcji zdalnych i dostosowany do konkretnej sytuacji, a nie obowiązkowy bez względu na towarzyszące transakcji okoliczności przyczyni się do rozwoju systemów zapobiegania fraudom. Dostawcy płatności konkurują obecnie nie tylko ceną, ale również jakością świadczonych usług, na te jakość składa się skuteczność zapobieganie fraudom przy jednoczesnym zachowaniu zadawalającego odbiorcę poziomu konwersji. Decyzja w przedmiocie zastosowania silnego uwierzytelnienia powinna być uwarunkowana profilem klienta i jego zachowaniami, mogłaby brać pod uwagę min. następujące czynniki:

- wartością transakcji - scoring transakcji powinien uwzględniać typowe dla płacącego średnie wartości transakcji, nietypowym zachowaniem będzie np. zainicjowanie transakcji kilkukrotne przewyższającej wartość poprzednich zakupów użytkownika
- lokalizację klienta na podstawie numeru IP, lokalizację urządzenia mobilnego, lokalizację akceptanta - ogromne możliwości analityczne wiążą się z kategorią „lokalizacji" począwszy od porównywaniu IP urządzenia z którego inicjowana jest płatność z miejscem wydania instrumentu płatniczego (np. karta wydana w Polsce vs. transakcja zainicjowana w Ghanie), a kończąc na monitorowaniu typowych cech kupujących w danym sklepie internetowym (np. przewaga kart wydanych przez lokalnych wydawców vs. zainicjowanie transakcji z wenezuelskiego numeru IP),
- zachowania charakterystyczne dla danej branży (np. sklepy jubilerskie, z elektroniką czy jedzeniem, biletami na transport publiczny) – które różnią się średnią wartością transakcji (np. transakcja w sklepie z biżuterią będzie kilkadziesiąt, kilkaset razy wyższa niż w podmiocie obsługującym on-linowe zakup biletów komunikacji miejskiej)
- zachowania związane daną metodą dostawy towaru (elektroniczna lub standardowa wysyłka) – np. zakup kodów do gier może nieść wyższe ryzyko niż sprzedaż pudełkowych produktów zawierających gry na nośnikach DVD.
- urządzenia jakich używa klient:
  - komputer stacjonarny – pliki cookies, „device fingerprinting" lub osobiste certyfikaty,
  - urządzenia mobilne (smatphon, tablet lub smartwatch) – unikatowy ID aplikacji mobilnej (jeśli jest) lub ID urządzenia,
  - inne urządzenia (jak telewizor lub lodówka) – unikatowy ID urządzenia.

Powyższe czynniki analizowane pojedynczo lub łącznie pozwalają na monitoring transakcji i zachowań klientów, tak aby wykrywać wszelkie nienaturalne zachowania dla których koniecznym może być wywołanie silnego uwierzytelnienia.

Stoimy także na stanowisku, że monitorowanie wielu czynników związanych z profilem klienta i jego zachowaniami powinno być uważane jako „samodzielny element będący cecha klienta (inherence) ". W przeciwieństwie do niektórych sposobów uwierzytelnienia (np. ograniczone w czasie kody SMS, które mogą być skompromitowane poprzez kradzież telefonu czy niechciane oprogramowanie) wzór zachowania klienta nie może być łatwo i szybko zmieniony.

- **Czy macie jakiekolwiek wątpliwości odnośnie listy wyłączeń zawartej w Rozdziale 2 propozycji regulacyjnych standardów technicznych w scenariuszu, w którym dostawcy usług płatniczych nie mogą stosować silnego uwierzytelnienia w przypadku transakcji, które spełniają kryteria sformułowane w wyłączeniu?**

Zgodnie z decyzją EBA aby "nie proponować wyłączeń opartych na analizie ryzyka transakcji" limity wymuszające silne uwierzytelnienie klienta ustalone są na bardzo niskim poziomie (10 Euro dla zdalnych transakcji elektronicznych). Aktualna treść regulacyjnych standardów technicznych nie jest dostosowana do warunków zmieniającego się rynku, jest mało elastyczna. Jest to zatem istotna przeszkoda biznesowa dla rozwoju dostawców usług płatniczych, gdyż nie pozwala ona na różnicowanie dostawców w oparciu wygodniejsze, prostsze czy bezpieczniejsze „user experience". Tak niski limit wpłynie negatywnie na wszystkie podmioty działające na rynku ecommerce łącznie z konsumentami, gdyż robienie zakupów on-line będzie wysoce nieprzyjazne dla użytkownika. Możemy być pewni, że rynek płatności rozwinie nowe funkcjonalności i usługi, które będą wiązać się z nowymi rodzajami ryzyka. Sztywne reguły (jak limit 10 Euro) nie znajdą zastosowania w przypadku tych nowych ryzyk, dlatego też sugerujemy aby zostawić dla uczestników rynku pewne ramy dowolności w stosowaniu silnego uwierzytelnienia klienta. Dodatkowo jesteśmy zdecydowanie przeciwko ograniczaniu dopuszczalnych zasad (trusted beneficiaries exemptions) tylko do transakcji kartowych. W *Rekomendacjach dotyczących bezpieczeństwa płatności internetowych* przygotowanych przez EBA "whitelisting" związane jest z transakcjami płatniczymi generalnie, a nie tylko przelewami („credit transfer"). Wprowadzenie ograniczenia tylko dla płatność typu „credit transfer" jest niezrozumiałe, jako że rynek płatniczy jest bardziej zróżnicowany, a przelew jest tylko jedną z możliwych form przekazania środków przez płacącego. Dodatkowo chcemy zwrócić uwagę iż, nie znajdujemy uzasadnienia dla wprowadzenia limitów wysokości 10 i 100 Euro, a ni przyczyny dlaczego dla zbliżeniowych transakcji kartowych zaproponowano kwotę 50 Euro dla pojedynczej transakcji mimo, iż w ocenie wielu ekspertów z tym rodzajem transakcji wiąże się wyższe ryzyko niż w przypadku transakcji w środowisku internetowym.

- Czy zgadzacie się z argumentacją EBA dotyczącą wymagań dla wspólnego i bezpiecznego otwartego standard komunikacji do celów identyfikacji, autentykacji, notyfikacji i informowania zawartych w Rozdziale 4 propozycji regulacyjnych standardów technicznych.

W odniesieniu do ogólnych standardów komunikacji występujących w środowisku internetowym (takich jak HTTP, HTTPS, TLS I SSL) podzielamy stanowisko EBA ("zbyt mało szczegółowe do komunikacji"). Ale aby zapewnić rynkowi odpowiedni poziom pewności EBA powinna uwzględnić te propozycje przynajmniej w preambule do regulacyjnych standardów technicznych.

W nawiązaniu do propozycja EBA, aby stworzyć standardy komunikacji na bazie wymagań międzynarodowych lub europejskich organizacji standaryzacyjnych, chcemy podkreślić, że w niektórych państwach (włączając w to Polskę) już teraz możemy znaleźć rozwiązania pozwalające na komunikację pomiędzy dostawcami usług płatniczych. Dlatego też zdecydowanie uważamy, że powinno być możliwym rozwijanie lokalnych (tj. w ramach danego państwa) standardów także bazujących na ISO 20022.