



OPEN
BANKING

OTWARTA BANKOWOŚĆ

Wydawcy raportu



ZWIĄZEK BANKÓW POLSKICH



Centrum Prawa Bankowego i Informacji
www.cpb.pl



aleBank.pl

OTWARTA BANKOWOŚĆ

Raport przygotowany przez
Związek Banków Polskich
oraz Centrum Prawa Bankowego i Informacji

© Copyright by Związek Banków Polskich

© Copyright by Centrum Prawa Bankowego i Informacji



ZWIĄZEK BANKÓW POLSKICH



Centrum Prawa Bankowego i Informacji
www.cpb.pl

Warszawa, październik 2020

Wydawnictwo Centrum Prawa Bankowego i Informacji



GFT POLAND



BREAKTHROUGH

Partner of the Year

2019

Twój biznes w rękach ekspertów

Szymon Kaczmarczyk
Client Unit Executive Poland & Asia Pacific

Globalne doświadczenie

- 1 Rozwiązania technologiczne dla największych banków inwestycyjnych i detalicznych
- 1 Zespół 800 ekspertów w Polsce i 6000 w 15 krajach świata
- 1 Star Performer wg Everest Open Banking IT Services PEAK Matrix® Assessment 2020

Eksperci najwyższej klasy

- 1 Komercyjne realizacje w obszarach AI, Cloud, Blockchain, Big Data
- 1 Niemal 200 certyfikatów AWS, Google i Azure

gft.com/pl

Silne partnerstwa

- 1 AWS Advanced Consulting Partner
- 1 Google Cloud EMEA Breakthrough Partner of the Year
- 1 Microsoft Gold Partner

- Optymalizacja i zarządzanie platformami core banking
- Migracja do środowisk chmurowych
- Tworzenie architektury danych
- Zapewnianie zgodności regulacyjnej rozwiązań IT
- Systemy kontroli ryzyka i przeciwdziałania oszustwom
- Kompleksowe narzędzia front office

SPIS TREŚCI

Od wydawcy	7
Czym jest open banking? Wprowadzenie do tematyki otwartej bankowości i opis rynku	8
Czym jest open banking?	11
Bankowość jako usługa	11
Po co bankom fintechy?	12
Nowe usługi płatnicze.....	13
AIS – usługa dostępu do informacji o rachunku	13
Zakres usługi AIS.....	14
Informacje o rachunku a dane osobowe i szczególnie chronione dane dotyczące płatności	15
Screen scraping, czyli AIS przed pojawieniem się open bankingu	15
PIS – usługa inicjowania płatności.....	16
Usługi spełniające rolę PIS przed pojawieniem się open bankingu	17
Modele wykorzystania usług płatniczych w biznesie	18
TSP – dostawcy usług technicznych.....	19
Ramy prawne open bankingu	19
SCA a open banking	22
Czy dostawcy rachunków płatniczych mogą różnicować podejście wobec różnych TPP?	23
Czy do świadczenia usług open bankingu potrzebna jest licencja?	23

Standardy dla otwartej bankowości w Europie	24
Dlaczego API (i ich standaryzacja) są ważne	26
Rekomendacje PolishAPI	26
Case studies – wybrane możliwości wykorzystania otwartej bankowości.....	27
Polscy dostawcy usług otwartej bankowości	30
Banki wykorzystujące rozwiązania otwartej bankowości	30
Podmioty znajdujące się na liście dostawców świadczących usługę dostępu do informacji o rachunku.....	31
Krajowe instytucje płatnicze	32
Rodzaje dostawców usług płatniczych.....	33
Wybrani dostawcy świadczący usługi otwartej bankowości w UE	34
Open banking na świecie.....	36
Wyniki ankiety.....	43
Zakończenie.....	49
W kierunku PSD 3.....	50
GAFA – nowi gracze na rynku finansowym.....	51
Nowoczesne API jako narzędzie komunikacji wewnętrznej i na zewnątrz w bankach – case studies	52
Rok bankowości otwartej: wygrywają tradycyjni gracze	58
Bank w rzeczywistości PSD2	64
Open banking a nadużycia, czyli jak bezpiecznie otwierać banki.....	68
Open banking – czyli dwie i pół usługi + API.....	72

MIĘDZYNARODOWA WIRTUALNA KONFERENCJA

BEYOND TOMORROW

BE CURIOUS. INNOVATE FAST. GAIN RESILIENCE.

23-25 listopada 2020

23 listopada - Data Science Day

24 listopada - Industry Day

25 listopada - Executive Experience Day

Cyfryzacja przyspiesza. Z nami będziesz na bieżąco.
Zapraszamy na konferencję Beyond Tomorrow, podczas której
podzielimy się dobrymi praktykami i pomysłami na wykorzystanie
zaawansowanej analityki i sztucznej inteligencji
w celu zrównoważenia negatywnych skutków pandemii,
zdobycia odporności na trudną do przewidzenia przyszłość
i zapewnienia organizacjom dynamicznego rozwoju.

Skorzystaj z możliwości networkingu w gronie praktyków cyfrowej transformacji
z Europy Środkowej, Rosji, Bliskiego Wschodu i Afryki.

W programie dedykowane sesje dla
bankowości, ubezpieczeń, telekomunikacji i handlu.

Konferencja jest bezpłatna i będzie prowadzona w języku angielskim.

Pełną agendę można znaleźć na stronie:

www.sas.com/cemea/beyondtomorrow

Zarejestruj się



#beyondtomorrow



OD WYDAWCY

Open banking to słowo, które na przestrzeni ostatnich kilkunastu miesięcy robi zawrotną karierę. Dzieje się tak nie tylko za sprawą dyrektywy PSD2, choć to ona położyła podwaliny pod otwarcie hermetycznych dotąd zasobów bankowych i dopuszczenie do korzystania z nich podmiotów trzecich, także z rozwijającego się dynamicznie sektora fintech. Open banking to przede wszystkim nieunikniona konsekwencja zmieniających się postaw i oczekiwań współczesnych konsumentów, dla których takie pojęcia, jak obsługa 24/7 czy one click stanowią jedynie słuszny kierunek ewolucji całej branży finansowej.

Przełomowym momentem dla otwartej bankowości, niezależnie od wcześniejszych, spontanicznych działań samych instytucji finansowych w tym zakresie, był początek obowiązywania PSD2, co w warunkach polskich nastąpiło 14 września 2019 r. Jedynie co dziesiąty przedstawiciel sektora finansowego, uczestniczący w ankiecie przeprowadzonej za pośrednictwem Związku Banków Polskich uważa, że otwarcie rynku dokonałoby się również i bez stymulacji ze strony regulatora. Taki stan rzeczy był wynikiem zarówno konkurencji wewnątrz branży, przez co poszczególne podmioty nie były zainteresowane udostępnianiem swych zasobów aktualnym lub potencjalnym rywalom, ale też i ryzyka regulacyjnego, związanego z dopuszczeniem podmiotów trzecich do wrażliwych danych, zgromadzonych w bankowych serwerowniach. Wszyscy mieli však w pamięci postępowania, prowadzone przez KNF w stosunku do instytucji finansowych, które jeszcze kilka lat temu zdecydowały się na zastosowanie screen scrappingu.

Jak wygląda sytuacja po kilkunastu miesiącach obowiązywania nowego prawa? Niniejszy raport stanowi zarówno próbę wyczerpującej odpowiedzi na to pytanie, jak też kompleksowego ujęcia problematyki open banking, ze szczególnym uwzględnieniem prezentacji nowatorskich modeli biznesowych, które mogły zaistnieć na rynku jedynie dzięki postanowieniom dyrektywy PSD2.

Podstawowym składnikiem otwartej bankowości jest oczywiście API, czyli interfejs programowania aplikacji, za pośrednictwem którego zachodzi komunikacja pomiędzy bankami a podmiotami trzecimi. Efektem wejścia

w życie PSD2 było opracowanie w kilku państwach członkowskich, w tym również w Polsce, jednolitych standardów specyfikacji technicznej dla API. W raporcie przedstawiamy przykłady takich rozwiązań, ukazując w telegraficznym skrócie ich genezę, a także zasięg stosowania danego standardu, jako że niektóre z nich, jak choćby Berlin Group, mają charakter transgraniczny. Szczególną uwagę poświęcamy rodzimemu rozwiązaniu Polish API, przypominając między innymi kluczowe dla wdrażania tego standardu rekomendacje.

Opracowanie zawiera także kompletną listę polskich instytucji finansowych, które zdecydowały się na wdrożenie rozwiązań z zakresu otwartej bankowości w praktyce, wraz z rodzajem udostępnianych przez nie usług. Cennym uzupełnieniem tego wykazu są charakterystyki przykładowych fintechów, zaangażowanych w obszar open banking na obszarze Unii Europejskiej. Są wśród nich podmioty z państw członkowskich, ale też i instytucje powstałe w innych regionach geograficznych, ze szczególnym uwzględnieniem Stanów Zjednoczonych. Warto też zapoznać się z informacjami na temat otwarcia rynku bankowego na obszarach, które nie podlegają pod reżimy PSD2. W raporcie znajdziemy podsumowanie sytuacji zarówno w państwach będących liderami transformacji cyfrowej, jak USA, Chiny, Japonia czy Korea Południowa, ale i w krajach takich, jak Australia, Nowa Zelandia i Nigeria.

Opracowanie nie ucieka od trudnych tematów, do jakich zaliczyć należy bez wątpienia wolniejszy niż zakładano rozwój open banking w polskich uwarunkowaniach. Przeprowadzone analizy, ze szczególnym uwzględnieniem cytowanego już badania przeprowadzonego w gronie bankowców, pozwalają wskazać najistotniejsze przeszkody i sformułować rekomendacje, w jaki sposób przyspieszyć ewolucję sektora w kierunku większej otwartości. To z kolei wydaje się niezbędne, zwłaszcza w obliczu coraz częściej postulowanej nowelizacji unijnych przepisów o świadczeniu usług płatniczych, określanych mianem dyrektywy PSD3.

Karol Móraski
redaktor prowadzący
„Miesięcznik Finansowy BANK”

Czym jest open banking?

WPROWADZENIE DO TEMATYKI OTWARTEJ BANKOWOŚCI I OPIS RYNKU



■ ARTUR BILSKI

Radca prawny, członek Centrum Badań nad Prawnymi Aspektami Technologii Blockchain oraz ekspert Instytutu Allerhanda. Od lat związany z polskimi i międzynarodowymi kancelariami prawnymi (ostatnio jako Counsel w Kochański & Partners, wcześniej Clifford Chance, Hogan Lovells), którym doradzał w obszarze regulacji finansowych i prawa nowych technologii. W ramach swojej praktyki związany był także z największymi bankami w Polsce – PKO BP, ING oraz Alior, przy czym w ostatnim z nich sprawował funkcję dyrektora Działu Obsługi Prawnej Biznesu. Zajmował również stanowisko dyrektora ds. prawnych w Ramp Network, wiodącej polskiej firmie zajmującej się płatnościami i technologią blockchain. Oprócz tego doradzał wielu instytucjom płatniczym, czy firmom związanym z nowymi technologiami, w tym AI. Jest autorem licznych publikacji z obszaru prawa finansowego, w tym Chambers Global Practice Guide on Securitisation of Financial Assets. Absolwent i pracownik naukowy Uniwersytetu Warszawskiego.



WSTĘP

Już ponad rok minął od wejścia w życie regulacji otwartej bankowości. Wydany w marcu 2019 r. przez Związek Banków Polskich i KPMG raport wskazywał, że wprowadzenie regulacji open banking w postaci dyrektywy PSD2, implementowanej do polskiego porządku prawnego w postaci znowelizowanej ustawy usługach płatniczych, oznacza, że „zajdą poważne zmiany na rynku płatności, tak w Polsce, jak i w Europie”. Niniejszy raport jest próbą odpowiedzi na pytanie, jak duże są to zmiany i w jaki sposób zareagował na nie sektor finansowy, a także jak zmieniło się podejście banków do samej idei open banking.

Na wstępie warto też odpowiedzieć sobie, jaki właściwie cel przyświecał ustawodawcy europejskiemu, który zdecydował się za pomocą szczególnej regulacji prawnej niejako „narzucić” uczestnikom rynku otwartą bankowość. Z pomocą przychodzi tu lektura preambuły do PSD2, odwołującej się także do zielonej księgi Komisji Europejskiej z dnia 11 stycznia 2012 r. zatytułowanej „W kierunku zintegrowanego europejskiego rynku płatności realizowanych przy pomocy kart płatniczych, przez Internet i za pośrednictwem urządzeń przenośnych”. Regulator europejski wprost stwierdził, że dotychczasowe regulacje były „zbyt wieloznaczne, zbyt ogólne lub po prostu przestarzałe”, co doprowadziło do „braku pewności prawa, potencjalnych ryzyk dla bezpieczeństwa w łańcuchu płatności oraz braku ochrony konsumentów”. Mówiąc ściślej – usługi takie jak przykładowo pozyskiwanie i agregacja przez osoby trzecie danych z rachunków bankowych w oparciu o dostęp udzielany przez tego klienta istniały już wcześniej. Nie gwarantowały one jednak dostatecznej ochrony

klienta, w związku z czym unijny legislator postanowił nieco „ucywilizować” te praktyki poprzez stworzenie dla nich ram regulacyjnych, które ponadto ułatwią świadczenie tego rodzaju działalności dzięki zwiększonemu dostępowi do infrastruktury bankowej.

PSD2 pozwoli wreszcie, dzięki usłudze inicjowania płatności, na ułatwiony sposób dokonywania przelewów bankowych. Do tej pory, w odróżnieniu od transakcji kartowych, dokonywanie płatności z wykorzystaniem tradycyjnego polecenia przelewu (a nie tzw. *pay-by-link*) było uciążliwe, wymagało bowiem manualnego uzupełnienia określonego katalogu danych, tj. nazwiska/nazwy odbiorcy i numeru jego rachunku płatniczego¹. Tymczasem dzięki inicjowaniu płatności przez dostawcę klient otrzyma gotowe dane do przelewu, który jedynie będzie musiał zatwierdzić, dokonując autoryzacji, co zapewnia dużą wygodę i bezpieczeństwo². Z kolei zaletami dla sprzedawców mogą być niższe koszty (brak opłaty interchange oraz innych opłat mających zastosowanie do transakcji kartowych) oraz relatywnie trudniejsze, w porównaniu do transakcji kartowych, cofnięcie już zleconej transakcji.

Celem niniejszego raportu jest przedstawienie czytelnikom krótkiego, praktycznego podsumowania istotnych zagadnień związanych ze środowiskiem otwartej bankowości i nowymi usługami płatniczymi, które wchodzi w jego skład. Jego lektura powinna umożliwić czytelnikowi:

- ▶ przyswojenie tego, czym jest open banking;
- ▶ zrozumienie funkcjonowania nowych usług płatniczych;

- ▶ zapoznanie się z zastosowaniami biznesowymi open banking;
- ▶ opanowanie podstawowych kwestii prawnych i technicznych, istotnych z punktu widzenia open banking; oraz
- ▶ poznanie działających na rynku polskim i europejskim największych dostawców świadczących usługi otwartej bankowości.

Opracowanie to kierowane jest przede wszystkim do uczestników rynku finansowego, w tym banków, dostawców usług płatniczych i podmiotów z nimi współpracujących, a także do wszystkich innych osób, w tym klientów, którzy pragną dowiedzieć się więcej o tym, jak funkcjonuje system otwartej bankowości. Autor starał się w sposób możliwie przystępny dokonać opisu praktycznych zagadnień związanych z open bankingiem, tak aby raport był wartościową lekturą zarówno dla czytelników, którzy dopiero poznają, czym jest otwarta bankowość, jak i dla tych już bardziej zaawansowanych.

Raport nie opisuje kompleksowo wszystkich kwestii związanych ze świadczeniem usług otwartej bankowości, tak technicznych, jak prawnych. Jego rolą jest raczej przybliżenie czytelnikowi zainteresowanemu pojęciem otwartej bankowości sposobu jej działania oraz funkcjonowania rynku. Osoby zainteresowane poszczególnymi aspektami open banking autor odsyła do dedykowanych publikacji Związku Banków Polskich oraz Komisji Nadzoru Finansowego.

W niniejszym dokumencie pojęcie „open banking” i „otwarta bankowość” są stosowane wymiennie. O ile to drugie jest z oczywistych względów bardziej poprawne językowo, to jednak w użyciu pozostaje przede wszystkim angielskie wyrażenie „open banking” i to głównie nim autor posługuje się w tej publikacji.

Jednocześnie, autor pragnie podziękować założycielom i pracownikom firmy Ramp Network, z którą miał okazję w przeszłości współpracować jako jeden z członków zespołu. Dzięki temu doświadczeniu autor miał okazję zetknąć się z otwartą bankowością i poznać prawne, biznesowe i techniczne uwarunkowania branży open banking w Polsce i na świecie, jak również mieć do czynienia z otwartą bankowością „od kuchni”.

¹ Wymogi w tym zakresie określa Rozporządzenie Parlamentu Europejskiego Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006 (dostępne na stronie: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32015R0847>).

² Dla porównania, w transakcjach kartowych stosuje się wyrażenia CIT (ang. Customer Initiated Transactions) i MIT (ang. Merchant Initiated Transactions). Te pierwsze oznaczają transakcje kartowe inicjowane bezpośrednio przez klienta, te drugie zaś – inicjowane w imieniu klienta przez akceptanta (najczęściej posiadającego terminal płatniczy sprzedawcy, w którego sklepie klient płaci kartą). Przykładem tych pierwszych może być zwyczajna płatność kartą, tych drugich zaś – zgoda na obciążenie karty przez akceptanta w sposób cykliczny (np. powtarzające się comiesięczne opłaty z tytułu karnetu).

CZYM JEST OPEN BANKING?

Mówiąc najprościej, otwarta bankowość to system (na który składają się regulacje prawne i technologia), który umożliwia uprawnionym podmiotom trzecim, za zgodą klienta, dostęp do określonych funkcjonalności infrastruktury bankowej (konta bankowego klienta) za pomocą dedykowanych API (interfejsów programistycznych rządzących wzajemnym komunikowaniem się aplikacji). W wydaniu PSD2 dostęp ten może opierać się na jednym z dwóch elementów:

- 1) pozyskaniu informacji o rachunku (TPP jako dostawca uzyskuje od banku prowadzącego rachunek³ np. dane o transakcjach użytkownika), czyli usługi AIS;
- 2) poleceniu bankowi wykonania określonej operacji z konta klienta (TPP jako dostawca „zleca” bankowi wykonanie polecenia przelewu o określonych parametrach), czyli usługi PIS.

TPP (ang. *Third Party Provider*) – jest to dosłownie „dostawca będący stroną trzecią”, czyli podmiot trzeci świadczący nowe usługi płatnicze wynikające z dyrektywy PSD2 (AIS lub PIS). Duża część TPP to podmioty z sektora fintech, choć oczywiście usługi te mogą być też świadczone np. przez bank, który występuje wówczas jako TPP.

Open banking to zatem każde z poniższych:

- ▶ prawo;

- ▶ technologia; oraz
- ▶ system wzajemnych powiązań pomiędzy bankami i dostawcami usług nowego typu opierających się na infrastrukturze bankowej,

ale przede wszystkim open banking to sieć produktów tworzonych przez korzystające z tych rozwiązań innowacyjne firmy działające na rynku finansowym (tzw. fintechy), które wdrażają je w sposób pozwalający na wygodniejsze, szybsze i bezpieczniejsze

Bankowość jako usługa (BaaS – *Banking as a Service*)

Koncepcja „bankowości jako usługi” wywodzi się od pojęcia SaaS (*Software as a Service*, czyli oprogramowanie jako usługa), które oznacza model korzystania z oprogramowania, gdzie to dostawca odpowiada za utrzymanie tego oprogramowania (najczęściej funkcjonującego w chmurze obliczeniowej) i je w pełni kontroluje, udostępniając je użytkownikowi, zaś użytkownik korzysta z niego, łącząc się np. przez internet. W skrócie rozwiązanie SaaS-owe można opisać jako usługę polegającą na umożliwieniu użytkownikowi korzystania z gotowego oprogramowania (użytkownik otrzymuje w pakiecie aktualizacje, serwis i utrzymanie) dostępnego za pośrednictwem (najczęściej) internetu.

W nieco podobny sposób funkcjonuje model BaaS, który należy przeciwstawić klasycznej bankowości. W modelu BaaS usługa bankowa, dostarczana przez internet, miałaby być dostępna na żądanie użytkownika i pozwalać na łatwą realizację potrzeb, na które odpowiada klasyczna bankowość. Do potrzeb tych należą przede wszystkim możliwość przechowywania środków (usługa rachunku bankowego), dokonywania płatności (usługa polegająca na transferze środków pieniężnych pomiędzy uczestnikami rynku), a w dalszej kolejności także finansowania. Otwarta bankowość i wykorzystanie nowych usług płatniczych, instytucji pieniądza elektronicznego czy infrastruktury zapewnianej przez sektor fintech pozwalają na realizację BaaS w dużej mierze z pominięciem banków i w ułatwiony z punktu widzenia klienta sposób. W tym modelu TPP, korzystając z już istniejących infrastruktur bankowych, oferowałyby szeroką paletę usług dotychczas oferowanych niemal wyłącznie przez banki. Należy tu jednak pamiętać o kwestii zabezpieczenia interesów klienta i zdeponowanych przez niego środków, a także specyfice sektora, który podlega licznym regulacjom oraz nadzorowi finansowemu. W dodatku np. założenie rachunku bankowego wiąże się z określonymi obowiązkami w zakresie identyfikacji i weryfikacji klienta przez podmiot prowadzący rachunek. O ile więc open banking jest krokiem w stronę BaaS, to trudno wyobrazić sobie już dziś sytuację, w której cały rynek miałby się przestawić z modelu biznesowego opartego na produktach na taki, którego podstawą miałyby być usługi (w rozumieniu BaaS).

³ W niniejszej publikacji autor wymiennie posługuje się wyrażeniami „bank” i formalnie bardziej poprawnym „dostawca prowadzący rachunek”.

niejsze płatności, jak również nowe sposoby wykorzystania informacji o rachunku. W szerszym ujęciu (wychodząc poza samo PSD2 i realia europejskie) open banking może także oznaczać szerszą współpracę banków i sektora fintech oraz możliwość otwartego korzystania z infrastruktury bankowej dla świadczenia usług płatniczych lub realizowania innych celów przewidzianych przez system.

Jednocześnie, aby mówić o wydajnym systemie otwartej bankowości konieczne jest łączne spełnienie wszystkich poniższych warunków:

- 1) dostępność, rozumiana jako możliwość wykorzystania infrastruktury bankowej przez podmioty trzecie bez nadmiernych barier wejścia i w sposób możliwie równy dla całego rynku, najlepiej nieodpłatnie; praktyka pokazuje, że partykularne interesy różnych uczestników rynku i trudność w oddolnym wypracowaniu jednolitych standardów oznaczają, że dla efektywnego spełnienia warunku dostępności konieczne jest najczęściej (przynajmniej w obecnych realiach rynkowych) powołanie ogólnorynkowych standardów regulacyjnych (w przypadku Unii Europejskiej PSD2), które pozwolą

na wypracowanie spójnego podejścia; równie ważne jak samo powołanie stosownej regulacji prawnej jest jednocześnie stworzenie i udostępnienie całemu rynkowi odpowiednich ram technicznych (standardu API), dających szansę na praktyczne powołanie do życia aplikacji umożliwiających klientowi skorzystanie z otwartej bankowości;

- 2) bezpieczeństwo, rozumiane jako istnienie mechanizmów i narzędzi zapewniających ochronę przed oszustwami i bezpieczne rozliczanie transakcji – w ramach europejskiej otwartej bankowości elementem zapewniającym jego spełnienie jest SCA, czyli silne uwierzytelnienie klienta;
- 3) kontrola, rozumiana jako z jednej strony wiarygodność dostawców usług płatniczych, z drugiej zaś bieżący nadzór i monitorowanie ich działalności pod kątem zgodności z prawem (zapewniana przez nadzór europejski oraz krajowy – w przypadku Polski Komisję Nadzoru Finansowego, jak również odpowiednie wymogi rejestracyjne lub licencyjne i obowiązki, jakie musi spełnić każdy, kto chce ubiegać się o status autoryzowanego dostawcy; ponadto PSD2 przewiduje wiele dodatkowych mechanizmów bezpieczeństwa, takich jak np. obowiązek posiadania przez dostawcę ubezpieczenia na wypadek pojawienia się roszczeń klientów).

Po co bankom fintechy?

Czy tradycyjne banki mogą skorzystać na współpracy z innowacyjnymi firmami z sektora finansowego? Odpowiedź jest oczywista – jak najbardziej tak! Z jednej strony możliwe jest postrzeganie TPP jako konkurencji dla tradycyjnych banków, z drugiej same banki wiele mogą zyskać na tworzeniu z fintechami wspólnych inicjatyw, które mogą pozwolić na poszerzenie oferty o kolejne produkty i przyciągnięcie nowych klientów.

Trzeba też powiedzieć, że co do zasady banki i fintechy działają w nieco innych niszach. Wynika to m.in. z faktu, że banki z różnych powodów, zarówno regulacyjnych, jak i operacyjnych czy wynikających z polityki zarządzania określonymi ryzykami, nie mogą (a często także nie chcą) rozszerzać swojej działalności na obszary, w których działa branża fintech. Przykładem może być działalność AISP-ów, które są w stanie wykorzystywać pozyskane informacje o rachunku do wykonywania innych czynności biznesowych, niekoniecznie nawet związanych ściśle z sektorem finansowym (przykład: kierowanie do klienta dedykowanych reklam czy promocji opartych na informacjach o jego dotychczasowych wydatkach)⁴. Oznacza to, że teza o „konkurowaniu” banków i fintechów w większości przypadków wcale nie musi być prawdą, a oba światy mogą wiele zyskać na wzajemnej współpracy.

⁴ Więcej na ten temat w części opisującej zakres usługi AIS.

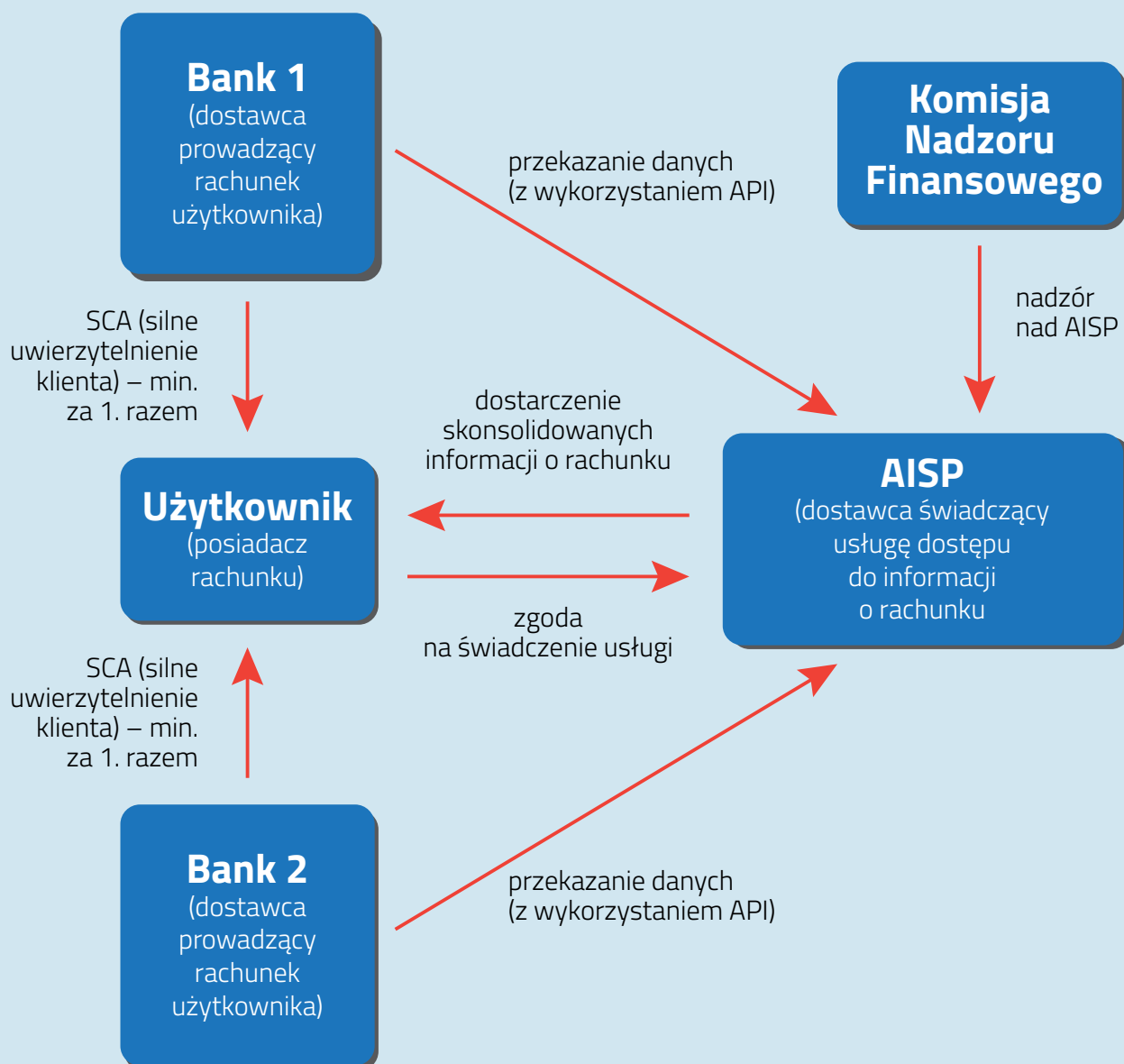
NOWE USŁUGI PŁATNICZE

Nowe usługi płatnicze to:

- ▶ **AIS (ang. Account Information Service)**, czyli usługa dostępu do informacji o rachunku (można ją porównać do „podglądania” rachunku klienta prze osobę trzecią, która otrzymuje określone dane normalnie widoczne jedynie dla użytkownika w ramach interfejsu bankowości elektronicznej). W skrócie polega ona

na możliwości uzyskania przez podmiot regulowany (AISP – *account information service provider*), za zgodą posiadacza rachunku, dostępu do określonych informacji widocznych dla tego klienta w ramach jednego lub kilku rachunków, u tego samego lub kilku dostawców. Zaliczają się do nich m.in. saldo rachunku czy wykonane operacje, ale nie szczególnie chronione dane dotyczące płatności. Podmioty

świadczące tego rodzaju usługę mogą np. oferować integratory rachunków bankowych, pozwalające na wygodne zarządzanie kilkoma rachunkami bankowymi za pomocą jednej aplikacji. Ponadto możliwe jest również, dzięki pozyskanym danym, świadczenie zupełnie nowego rodzaju usług, takich jak np. scoring czy ocena ryzyka wykorzystująca dane z rachunków – i wiele innych.



Zakres usługi AIS

Komisja Nadzoru Finansowego w komunikacie z 44. Posiedzenia Komisji Nadzoru Finansowego w dniu 14 października 2019 r.⁵ wskazała, że usługa AIS polega na „dostarczaniu posiadaczom rachunków płatniczych skonsolidowanych informacji o tych rachunkach”. Kluczowym elementem tak skonstruowanej definicji jest ograniczenie możliwości świadczenia usługi AIS do przekazywania użytkownikom informacji o ich własnych rachunkach (co oznacza zawężenie głównie do budowania integratorów rachunków).

Nie sposób zgodzić się z taką interpretacją. Jej przyjęcie oznaczałoby wykluczenie z rynku polskiego możliwości świadczenia wielu rodzajów usług. Ponadto, brak zarówno w ustawie, jak i dyrektywie, przesłanek do uznania, że usługa AIS może być świadczona jedynie względem posiadacza rachunku. Sam art. 3 ust. 6 ustawy o usługach płatniczych stwierdza, że „Usługa dostępu do informacji o rachunku oznacza usługę online polegającą na dostarczaniu skonsolidowanych informacji dotyczących (...) rachunku płatniczego użytkownika”. Nie zostało tutaj określone, komu te informacje powinny zostać dostarczone, nie można więc stwierdzić, że dotyczy to jedynie użytkownika.

Stanowisko, że AISP może przekazywać dane o rachunku do osób trzecich (a nie tylko do użytkownika) podziela również EBA (Europejski Urząd Nadzoru Bankowego), który w ramach swojego stanowiska⁶ wyraził opinię, że AISP mogą przekazywać pozyskane informacje o rachunku także do osób trzecich i wciąż stanowi to usługę płatniczą w rozumieniu PSD2⁷. Jednocześnie, trzeba pamiętać, że konieczne jest stosowne opisanie świadczonej usługi, tak żeby klient miał świadomość, w jaki sposób są wykorzystywane te dane.

Ponadto AISP może też świadczyć usługi inne niż tylko usługa AIS, może więc wykorzystywać informacje o rachunku w inny sposób, niż tylko dostarczanie skonsolidowanej informacji o rachunkach online. Świadcząc o tym wprost przepisy ustawy o usługach płatniczych, która jasno stwierdza, że taki dostawca „może prowadzić działalność gospodarczą inną niż świadczenie usług płatniczych”⁸.



Usługa AIS może być świadczona przez jeden z trzech rodzajów podmiotów (nazywanych dalej AISP-ami):

- ▶ bank świadczący tę usługę płatniczą;
- ▶ instytucję płatniczą, której licencja obejmuje AIS; albo
- ▶ AISP świadczący wyłącznie usługę dostępu do informacji o rachunku, czyli nieświadczący żadnej innej usługi płatniczej – podmiot tego typu operuje na szczególnych zasadach (m.in. nie wymaga licencji, a jedynie wpisu do rejestru, nie stosuje się też do niego niektórych przepisów).

W przeciwieństwie do AIS, dla świadczenia usługi PIS konieczna jest licencja bankowa albo instytucji płatniczej.

5 Dokument dostępny na stronie: https://www.knf.gov.pl/o_nas/komunikaty?articleId=67404&p_id=18.

6 Odpowiedź udzielona przez EBA na pytanie o sygn. 2018_4098 w ramach EBA Single Rulebook, tekst odpowiedzi dostępny jest w języku angielskim na stronie: https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4098.

7 Ang. „Articles 4(16) and 67(1),(2) PSD2 do not require that the account information service provider (AISP) provides the consolidated information to the payment service user (PSU) in order for the service to constitute an 'account information service' according to PSD2. The AISP may therefore transmit the consolidated information to a third party with the PSU's explicit agreement. Regarding the use made by any third party of the consolidated information transmitted, other provisions of EU law may apply, for instance the General Data Protection Regulation (EU) 2016/679 (GDPR).”.

8 Art. 117a ust. 2 ustawy oraz art. 18 ust. 1 lit. c PSD 2 (który odnosi się szeroko do instytucji płatniczych).

Informacje o rachunku a dane osobowe i szczególnie chronione dane dotyczące płatności

Jak wskazano powyżej, AISP nie mają możliwości uzyskania związanych z rachunkami płatniczymi „szczególnie chronionych danych dotyczących płatności”. Mowa tu o danych, które mogą być wykorzystywane do dokonywania oszustw. W szczególności chodzi o indywidualne dane uwierzytelniające, takie jak np. hasło czy numer klienta. PSD2 wyłącza jednak z tej kategorii imię i nazwisko oraz numer rachunku, te dane można więc z pewnością przekazywać AISP-om.

Powyższa definicja jest otwarta, co oznacza, że wchodzi w nią wiele rodzajów informacji. Zaliczyć do nich można, oprócz wspomnianych już danych uwierzytelniających, informacje takie, jak np. dane karty płatniczej (mogą posłużyć do oszukańczej transakcji).

Podobna sytuacja dotyczy pozyskiwania przez dostawców świadczących usługi otwartej bankowości danych o użytkowniku (jak np. danych adresowych) czy danych kontaktowych, takich jak adres czy telefon. O ile te dane same w sobie nie pozwalają na dokonanie oszustwa (aczkolwiek w pewnych warunkach ułatwić jego przeprowadzenie), to nie są też niezbędne dla samego świadczenia usługi płatniczej i w związku z tym zdaniem EBA (Europejskiego Urzędu Nadzoru Bankowego, ang. European Banking Authority) nie powinny być przekazywane⁹. Jednocześnie TPP staje się administratorem pozyskiwanych danych osobowych, co oznacza konieczność dostosowania się do określonych wymogów RODO¹⁰.

⁹ Pkt. 27 opinii EBA z 13 czerwca 2018 dot. wdrożenia RTS, nr. EBA-Op-2018-04; dokument jest dostępny na stronie: <https://eba.europa.eu/eba-publishes-opinion-on-the-implementation-of-the-rtis-on-strong-customer-authentication-and-common-and-secure-communication>.

¹⁰ Tj. 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, którego pełen tekst dostępny jest na stronie: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32016R0679>.

Screen scraping, czyli AIS przed pojawieniem się open bankingu

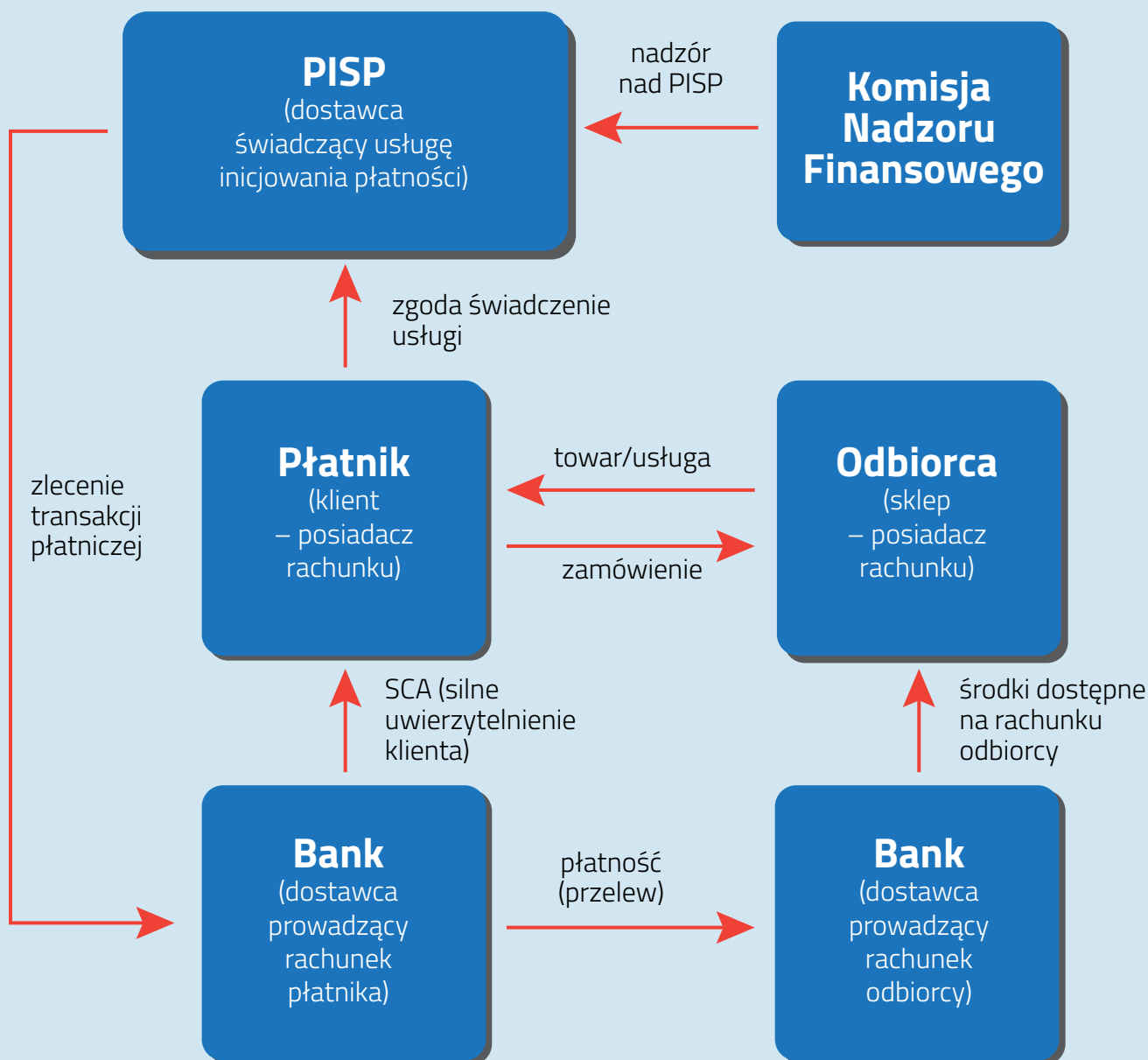
Jeszcze przed wejściem w życie PSD2 i pojawieniem się usługi AIS różne działające na rynku firmy technologiczne pozyskiwały informacje o rachunku klienta, wykorzystując tzw. screen scraping (zdrapywanie ekranu). Polega to na wykorzystaniu danych uwierzytelniających otrzymanych od klienta do zalogowania się przez dostawcę tak, jakby był on klientem. Po takim zalogowaniu aplikacja dostawcy jest w stanie automatycznie „ściągać” określone dane widoczne w serwisie bankowości elektronicznej.

Szerokie stosowanie screen scrapingu, będące zresztą jednym z powodów wprowadzenia PSD2, spotkało się w Polsce z wyraźną reakcją nadzorca finansowego. Urząd Komisji Nadzoru Finansowego w komunikacie z 14 lipca 2014 r. opowiedział się przeciwko wykorzystywaniu tej metody, wskazując klientom, że podawanie loginu i hasła do swojego konta bankowego stanowi naruszenie reguł korzystania z rachunków bankowych i może prowadzić do utraty możliwości reklamowania ewentualnych nieautoryzowanych transakcji wykonanych z rachunku klienta.

► **PIS (ang. Payment Initiation Service)**, czyli usługa inicjowania płatności, która w uproszczeniu polega na możliwości wydawania bankowi przez podmiot regulowany (PISP – *payment initiation service provider*), za zgodą klienta, wiążących instrukcji dokonania polecenia przelewu o określonych

parametrach. Podmioty oferujące tego rodzaju usługę mogą zastąpić istniejące usługi przekazywania płatności oraz je uprościć (nie będzie potrzeby manualnego wykonywania płatności przez użytkownika, a jedynie zatwierdzenie poprzez SCA płatności o określonych parametrach), przy zapew-

nieniu większego bezpieczeństwa i szybkości. Warto dodać, że powszechnie stosowane w Polsce metody płatności typu pay-by-link czy wykorzystywanie instrumentu w postaci blik w reszcie Europy są w dużej mierze nieznane – dzięki PSD2 płacenie w ten sposób stało się możliwe na całym kontynencie.



Usługi spełniające rolę PIS przed pojawieniem się open bankingu

Zanim pojawiły się usługi PIS, wiodącymi sposobami dokonywania płatności były (i wciąż jeszcze są) karty płatnicze oraz tradycyjne przelewy bankowe. Rynek, a zwłaszcza branża e-commerce, poszukiwały jednak wygodnych rozwiązań alternatywnych, stąd pojawienie się w Polsce podmiotów takich, jak PayU (a w Stanach Zjednoczonych PayPal czy później Venmo), które umożliwiły dokonywanie szybkich i bezpiecznych płatności np. w serwisach akcyjnych. Usługi te często wykorzystywały zresztą istniejącą infrastrukturę, co upodabnia je poniekąd do otwartej bankowości. Przykładowo. Oprócz tego, poczynwszy od 2015 r. klienci banków uczestniczących w systemie blik mogą korzystać również z tego rozwiązania płatniczego, pozwalającego na dokonywanie natychmiastowych płatności z wykorzystaniem aplikacji mobilnych.

Wprowadzie wspomniane rozwiązania nie są oparte na open bankingu i nie pozwalają na automatyzację płatności w sposób, jaki umożliwia usługa PIS, nie można jednak zapomnieć o oferowanej przez nie funkcjonalności, jaką jest szybkość. W przeciwieństwie do standardowego przelewu oferują one bowiem (podobnie jak transakcje kartowe i podobnie jak PIS) niemal natychmiastowe (przynajmniej z punktu widzenia klienta) rozliczenie transakcji, co sprawia się zwłaszcza w płatnościach w sklepach internetowych.

Oprócz wymienionych powyżej typów usług, PSD2 przewiduje również usługę potwierdzania środków na rachunku, czyli CAF (ang. *Confirmation on Availability of Funds*). Polega ona na potwierdzaniu przez dostawcę prowadzącego rachunek dostępności środków niezbędnych do wykonania określonej transakcji płatniczej. Bank (lub inny dostawca prowadzący rachunek) wskazuje w tym przypadku, na wniosek wydawcy instrumentu płatniczego opartego na karcie płatniczej, czy wymagana kwota jest dostępna (bez podawania całego salda i bez blokowania środków). Usługa ta może grać istotną rolę dla wydawców instrumentów płatniczych niebędących jednocześnie podmiotami prowadzącymi rachunek powiązany z instrumentem. Mogą oni dzięki jej zastosowaniu weryfikować w sposób uproszczony, czy rachunek, z którym powiązany jest dany instrument płatniczy, zawiera środki wymagane dla prawidłowego rozliczenia.



Instrument płatniczy – definicja

Zgodnie z ustawą o usługach płatniczych instrument płatniczy to „zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego”. Typowym przykładem instrumentu płatniczego jest karta płatnicza.

Modele wykorzystania usług płatniczych w biznesie

Poniższa lista przedstawia możliwe struktury służące świadczeniu na rzecz klienta końcowego usługi płatniczej:

- 1) Model bezpośredni – w tym modelu uprawniony dostawca, posiadający zezwolenia, infrastrukturę i zaplecze techniczne świadczy usługę płatniczą bezpośrednio na rzecz klienta końcowego, realizując swój własny produkt. Jest to najbardziej klasyczny model świadczenia usług płatniczych.

Przykład: instytucja płatnicza posiadająca zezwolenie na świadczenie usług AIS/PIS, prowadząca działalność gospodarczą polegającą na agregowaniu rachunków klienta

- 2) Model dostępowy/wspierający – w tym modelu dostawca ma możliwości prawne i techniczne oraz infrastrukturę pozwalającą na świadczenie usług płatniczych, jednak jego model biznesowy opiera się nie na tworzeniu nowych produktów dla klienta końcowego (np. agregatorów rachunków), lecz na wspieraniu innych podmiotów chcących takie usługi wykorzystywać. Może to polegać np. na pozyskiwaniu w ramach AIS informacji o rachunku, a następnie przekazywaniu ich na rzecz podmiotu trzeciego, który świadczy konkretną usługę, jaką może być usługa płatnicza (agregacja rachunków) albo usługa zupełnie innego typu. Model ten może być nazywany „dostępowym”, ponieważ wiele istniejących podmiotów licencjonowanych opiera swoją działalność przede wszystkim na zapewnianiu dostępu do API bankowych podmiotom trzecim.

- 3) Usługa świadczona przez zewnętrznego TPP – w tym modelu podmiot chcący wykorzystać rozwiązania open bankingowe w ogóle nie działa jako dostawca i w pełni powierza wykonywanie tych usług podmiotowi trzeciemu. Usługa płatnicza wykorzystywana w modelu biznesowym takiej firmy będzie świadczona przez dostawcę realizującego w ramach swojej działalności model bezpośredni (jeśli usługa płatnicza występuje jako dodatkowa

czynność) lub wspierający (jeśli usługa płatnicza jest trwale związana z oferowaną usługą podstawową).

Przykład: serwis e-commerce wykorzystujący zewnętrznego TPP posiadającego licencję instytucji płatniczej, który świadczy dla klientów usługę PIS, pozwalającą na usprawnienie płatności w serwisie.

Niezależnie od powyższego, warto wyszczególnić również dwa podtypy modeli dostawców, mogących świadczyć usługę w modelu bezpośrednim lub wspierającym:

- a) Model agencyjny (dostawca usługi płatniczej nie dysponuje licencją/wpisem do rejestru dostawców) – w tym modelu podmiot działa jako agent w imieniu podmiotu trzeciego posiadającego licencję TPP. Podmiot licencjonowany niejako „użycza” więc za opłatą swojej licencji podmiotowi trzeciemu, który może wówczas działać jako jego transparentny pośrednik, pod warunkiem spełnienia stosownych wymogów i wpisaniu na listę agentów. W odróżnieniu od modelu dostępowego usługa będzie tu świadczona na rzecz klienta przez agenta w imieniu TPP, nie zaś samodzielnie i bezpośrednio przez posiadające licencję TPP.
- b) Model wykorzystujący TSP¹¹ (dostawca usługi płatniczej nie dysponuje technologią) – w tym modelu dostawca posiada wprawdzie zezwolenie na prowadzenie działalności w obszarze usług płatniczych AIS lub PIS, brakuje mu jednak niektórych narzędzi technicznych pozwalających na integrację z bankowymi API (lub jest to z innych względów nieopłacalne). Wówczas wykorzystywany jest tzw. zewnętrzny TSP, czyli dostawca techniczny odpowiedzialny za zbudowanie i utrzymanie takich połączeń. Funkcjonowanie jako TSP nie wymaga żadnej licencji, jest to w skrócie firma technologiczna dysponująca możliwością zbudowania API dla takiego dostawcy i przyłączenia go do API bankowych.

¹¹ Ang. „Technical Service Provider”, czyli dostawca usług technicznych.

TSP

Powtarzając za ustawą, regulacja PSD2 nie dotyczy usług świadczonych przez dostawców usług technicznych (TSP), wspierających jedynie świadczenie usług płatniczych i niewchodzących w posiadanie środków pieniężnych. Odnosi się to w szczególności do usług przetwarzania i przechowywania danych, usług powierzenia i ochrony prywatności, usług przekazywania między płatnikiem a odbiorcą informacji o transakcji płatniczej, uwierzytelniania danych i podmiotów, dostarczania technologii informatycznych (IT) i sieci komunikacyjnych, dostarczania i utrzymania terminali i urządzeń wykorzystywanych do świadczenia usług płatniczych.

Jednocześnie, pomimo że AISP i PISP co do zasady również nie wchodzi w posiadanie środków pieniężnych¹², to wybrane przepisy dyrektywy (oraz ustawy o usługach płatniczych) dotyczą tych podmiotów i nie są one wyłączone z ich stosowania. Same usługi AIS i PIS mają zresztą charakter więcej niż tylko techniczny – każda z nich jest usługą płatniczą.

12 W stosunku do PISP jest to zresztą jeden z wymogów określonych przez art. 59r ust. 3 ustawy o usługach płatniczych: „Dostawca świadczący usługę inicjowania transakcji płatniczej (...) nie może wchodzić w posiadanie środków pieniężnych płatnika w związku ze świadczeniem usługi inicjowania transakcji płatniczej”.

RAMY PRAWNE OPEN BANKINGU

Głównymi aktami prawnymi określającymi założenia open banking w Polsce są PSD2 (oraz implementująca je ustawa o usługach płatniczych) oraz RTS.

Kluczowe akty prawne

PSD2 (ang. *Payment Services Directive 2*)¹³ – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywę 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE – dyrektywa określająca prawne ramy usług płatniczych (w tym otwartej bankowości).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych¹⁴ – polska ustawa stanowiąca implementację PSD2 do polskiego porządku prawnego (przepisy PSD2, będącego dyrektywą, co do zasady nie są stosowane bezpośrednio).

RTS – oprócz PSD2 i ustawy o usługach płatniczych szczególnie reguły określające wymogi prawne względem dostawców świadczących usługi płatnicze oraz np. wyłączenia od stosowania SCA (silnego uwierzytelniania klienta) określa rozporządzenie techniczne (tzw. RTS), czyli Rozporządzenie Delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji¹⁵.

Ponadto, z punktu widzenia rozporządzenia i prowadzenia działalności,

istotne dla podmiotów świadczących usługi płatnicze z zakresu otwartej bankowości są następujące rozporządzenia Ministra Finansów:

► dla AISP:

- 1) Rozporządzenie Prezesa Rady Ministrów z dnia 23 września 2019 r. w sprawie wpłat na pokrycie kosztów nadzoru nad dostawcami świadczącymi wyłącznie usługę dostępu do informacji o rachunku¹⁶, odnoszące się do wysokości opłat za pokrycie kosztów nadzoru ponoszonych przez TPP;
- 2) Rozporządzenie Ministra Finansów z dnia 31 lipca 2019 r. w sprawie

13 Tekst dostępny jest na stronie: <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32015L2366&from=PL#d1e1069-35-1>.

14 Tekst dostępny jest na stronie: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=W-DU20111991175>.

15 Tekst dostępny jest na stronie: <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32018R0389&from=EN>.

16 Tekst dostępny jest na stronie: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=W-DU20190001876>.

minimalnej sumy gwarancyjnej ubezpieczenia, sumy gwarancji bankowej, sumy gwarancji ubezpieczeniowej lub wartości innego zabezpieczenia roszczeń użytkownika, o których mowa w art. 117a ust. 3 ustawy o usługach płatniczych¹⁷, odnoszące się do wysokości ubezpieczenia (lub innego zabezpieczenia) jakie powinien posiadać AISP.

► dla PISP:

Rozporządzenie Ministra Finansów z dnia 31 lipca 2019 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia, sumy gwarancji bankowej, sumy gwarancji ubezpieczeniowej lub wartości innego zabezpieczenia roszczeń użytkownika, o których mowa w art. 61b ust. 1 ustawy o usługach płatniczych¹⁸, odnoszące się do wysokości ubezpieczenia (lub innego zabezpieczenia), jakie powinien posiadać PISP.

Oprócz wymienionych aktów prawnych dostawców usług open bankingu dotyczyć mogą również inne przepisy. Przykładem jest ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (która stanowi implementację dyrektywy AMLD V). Ustawa ta określa zakres obowiązków tzw. instytucji obowiązanych, do których zaliczają się także banki, instytucje płatnicze oraz AISP (co potwierdziły również organy nadzoru finansowego w państwach Unii Europejskiej, m.in. niemiecki BaFin¹⁹). W przypadku tych ostatnich może to budzić pewne kontrowersje, nie rozliczają one bowiem transakcji, a jedynie mają możliwość „wglądu” w dane o rachunku, które widzą zresztą również dostawcy rachunku płatniczego, sami będący instytucjami obowiązkanymi²⁰. Uzasadnieniem może być tu jednak fakt, że AISP może posiadać dostęp do danych z więcej niż jednego rachunku płatniczego (klient może mieć kilka rachunków w różnych bankach), a więc dysponować wiedzą, której żaden z dostawców rachunku płatniczego samodzielnie nie posiada.

Z punktu widzenia konkretnych przepisów odnoszących się do open bankingu można wyróżnić, w ramach odpowiednio ustawy o usługach płatniczych i RTS:

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych:

Art. 2 pkt. 4d ustawy²¹ – definicja PISP;

Art. 2 pkt. 4e²² – definicja dostawcy AIS innego niż AISP świadczący wyłącznie usługę dostępu do informacji o rachunku;

Art. 2 pkt. 4f – definicja AISP świadczącego wyłącznie usługę dostępu do informacji o rachunku;

Art. 2 pkt. 26aa²³ – definicja SCA;

Art. 3 ust. 1 pkt 7 i ust. 5²⁴ – definicja PIS;

Art. 3 ust. 1 pkt 8 i ust. 6²⁵ – definicja AIS;

Art. 59q–59t²⁶ – warunki świadczenia usług PIS i AIS;

Art. 60–61²⁷ oraz 64–64a – wymogi dla złożenia wniosku do KNF o wydanie zezwolenia na świadczenie usług płatniczych w charakterze instytucji płatniczej (odpowiednio – rejestracji AISP świadczącego wyłącznie usługę dostępu do informacji o rachunku);

17 Tekst dostępny jest na stronie: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001458>.

18 Tekst dostępny jest na stronie: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001459>.

19 Tekst konsultacji w tej sprawie dostępny jest na stronie: https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2018/dl_kon_0518_auas_gw.pdf?__blob=publicationFile&v=3.

20 Kontrowersje te pojawiły się zresztą także na rynku polskim, o czym pisała m.in. „Gazeta Prawna”: <https://serwis.gazetaprawna.pl/nowe-technologie/artykuly/1394612,restrikcyjnych-wymogow.html>.

21 Art. 4 pkt. 18 PSD 2.

22 Art. 4 pkt. 19 PSD 2.

23 Art. 4 pkt. 30 PSD 2.

24 Art. 4 pkt. 15 PSD 2.

25 Art. 4 pkt. 16 PSD 2.

26 Art. 66–67 PSD 2.

27 Art. 5 PSD 2.

Art. 61b²⁸ – szczególne warunki dotyczące obowiązku posiadania przez PISP ubezpieczenia, gwarancji bankowej lub ubezpieczeniowej albo innego zabezpieczenia roszczeń użytkownika;

Art. 117a–117e²⁹ – warunki wpisu do rejestru i funkcjonowania dostawców świadczących wyłącznie usługę AIS.

RTS:

Art. 4–9 – środki bezpieczeństwa przy stosowaniu SCA;

Art. 10 – wyłączenia od stosowania SCA wobec AISP;

Art. 30–35 – wymogi dotyczące otwartych standardów komunikacji, w tym interfejsów;

Art. 36 – wymiany danych, w tym wymogi dotyczące przekazywania danych przez PISP oraz reguły uzyskiwania dostępu do informacji o rachunku przez AISP.

Szczegóły dotyczące wymogów prawnych względem PISP oraz AISP, zarówno pod kątem uzyskania zezwolenia (rejestracji) szczegółowo opisuje na swojej stronie Komisja Nadzoru Finansowego (KNF):

- ▶ proces licencyjny dla krajowej instytucji płatniczej: https://www.knf.gov.pl/dla_ryнку/procesy_licencyjne/platniczy/krajowe_instytucje_platnicze
- ▶ rejestracja dostawcy (AISP) świadczącego wyłącznie usługę dostępu do informacji o rachunku:



https://www.knf.gov.pl/dla_ryнку/procesy_licencyjne/platniczy/AISP/Rejestracja_AISP

- ▶ podstawowe obowiązki AISP: https://www.knf.gov.pl/dla_ryнку/procesy_licencyjne/platniczy/AISP/Podstawowe_obowiazki_AISP

W ramach prowadzonego przez KNF programu edukacyjnego CEDUR została też wydana publikacja Kamila Leżonia pt. „Otwarta bankowość w świetle wymogów dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora fintech”³⁰, która w wyczerpujący sposób opisuje kluczowe wymogi RTS. Czytelników

zainteresowanych tematem autor odsyła do wspomnianej publikacji.

Warto w tym miejscu podkreślić też szczególną rolę KNF, która prowadzi postępowanie związane z uzyskaniem zezwolenia/wpisem do rejestru jako TPP. Ponadto KNF sprawuje nadzór zarówno nad bankami, jak i nad PISP-ami oraz AISP-ami, do jej zaleceń te podmioty są zobowiązane się stosować. W przypadku naruszenia warunków wymaganych prawem do prowadzenia działalności w charakterze dostawcy usług płatniczych KNF może przeprowadzić postępowanie kontrolne, wydać zalecenia dla podmiotu nadzorowanego, a nawet nałożyć na prowadzących działalność karę pieniężną czy zakazać prowadzenia tej działalności.

²⁸ Art. 5 ust. 2 PSD 2.

²⁹ Art. 33 PSD 2.

³⁰ Dostępna pod adresem: https://www.knf.gov.pl/?articleId=68606&p_id=18.

SCA a open banking

Wprowadzenie nowych usług płatniczych AIS i PIS nie jest jedyną kluczową zmianą wynikającą z PSD2. Innym niezwykle istotnym elementem jest wprowadzenie nowego mechanizmu silnego uwierzytelniania klienta, tzw. SCA (ang. *Strong Customer Authentication*). Dokonanie przez klienta uwierzytelnienia jest konieczne dla przeprowadzenia inicjacji transakcji płatniczej w ramach PIS, a w pewnym zakresie będzie też wymagane dla uzyskania dostępu do informacji o rachunku przez dostawcę AIS.

Na SCA składają się trzy elementy, z których co najmniej dwa różne muszą być spełnione, aby dokonać autoryzacji danej czynności:

- 1) wiedza (coś, co klient wie – np. hasło);
- 2) posiadanie (coś, co klient posiada – np. dedykowane urządzenie); oraz
- 3) cecha klienta (coś, czym klient jest – rolę tę może spełniać np. odcisk palca).

Typowym przykładem przeprowadzenia SCA może być więc np. wpisanie hasła na posiadanym przez klienta telefonie, który jest rozpoznawany przez system bankowości elektronicznej.

RTS, oprócz zwolnień dot. np. transakcji niskokwotowych³¹, przewiduje szczególne wyłączenia od SCA dla usługi AIS³². Z wyjątkiem uzyskania dostępu przez AISP po raz pierwszy, możliwe jest niestosowanie SCA przy uzyskiwaniu dostępu do informacji o rachunku, o ile nie minęło 90 dni od ostatniego uzyskania dostępu przez użytkownika albo ostatniego zastosowania SCA.

31 Tj. takich, gdzie kwota pojedynczej transakcji nie przekracza 30 euro, a transakcji od kiedy ostatnio przeprowadzono SCA było nie więcej niż 5 i nie przekroczyły one łącznie kwoty 100 euro.

32 Art. 10 RTS:

1. Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia wymogów określonych w art. 2 i w ust. 2 niniejszego artykułu, w przypadku gdy dostęp użytkownika usług płatniczych ogranicza się do dostępu do jednej z wymienionych niżej pozycji w trybie online lub do obu tych pozycji bez ujawniania szczególnie chronionych danych dotyczących płatności:

a) salda jednego wyznaczonego rachunku płatniczego lub większej liczby wyznaczonych rachunków płatniczych;

b) transakcji płatniczych przeprowadzonych w ciągu ostatnich 90 dni za pośrednictwem jednego wyznaczonego rachunku płatniczego lub większej ich liczby.

2. Do celów ust. 1 dostawcy usług płatniczych nie podlegają wyłączeniu z obowiązku stosowania silnego uwierzytelniania klienta, jeżeli spełniony jest którykolwiek z następujących warunków:

a) użytkownik usług płatniczych uzyskuje dostęp do informacji określonych w ust. 1 w trybie online po raz pierwszy;

b) minęło więcej niż 90 dni odkąd użytkownik usług płatniczych po raz ostatni uzyskał dostęp do informacji określonych w ust. 1 lit. b) w trybie online oraz odkąd ostatni raz zastosowano silne uwierzytelnianie klienta.

Czym jest „opcja fallback”?

Jednym z istotnych wymogów wprowadzonych dla banków przez RTS jest udostępnienie przez dostawców prowadzących rachunek mechanizmu rezerwowego pozwalającego TPP na korzystanie z klasycznego interfejsu dostępowego (zamiast tego przeznaczonego normalnie dla TPP). Korzystanie z niego jest możliwe w sytuacji awarii lub nieplanowanej dostępności zazwyczaj stosowanych kanałów dostępności. Celem wprowadzenia tej opcji (ang. *fallback mechanism*) jest zapewnienie nieprzerwanego dostępu TPP do określonych funkcjonalności rachunku bankowego w sytuacjach nadzwyczajnych.



Czy dostawcy rachunków płatniczych mogą różnicować podejście wobec różnych TPP?

Zgodnie z PSD2 oraz ustawą o usługach płatniczych świadczenia usług inicjowania płatności lub usług dostępu do informacji o rachunku nie można uzależniać od istnienia stosunku umownego pomiędzy dostawcami świadczącymi usługę inicjowania płatności a dostawcami usług płatniczych prowadzącymi rachunek do tego celu. Oznacza to, że dany bank (lub inny podmiot prowadzący rachunek) nie może „odmówić” współpracy z dostawcą usług płatniczych zawarcia umowy, uzależniając to od zawarcia wcześniej stosownej umowy lub wypłaty wynagrodzenia. Wpisuje się to w ideę otwartej bankowości, która z założenia ma umożliwiać dostęp do bankowych API na równych i przystępnych zasadach.

Nie oznacza to jednak, że banki nie mogą stosować odmiennego traktowania względem określonych podmiotów. Dotyczy to w szczególności AISP-ów. Z RTS-ów wynika bowiem, że dostawcy usług płatniczych „mogą nie stosować” (ang. *shall be allowed not to apply*) silnego uwierzytelniania klienta, z wyjątkiem sytuacji, gdy dane udostępniane są po raz pierwszy albo gdy minęło ponad 90 dni od ostatniego zastosowania SCA. Mogą, a więc nie muszą – czyli w wariancie alternatywnym SCA będzie wymagane. Ponadto, zgodnie z tą regulacją, AISP może pozyskiwać informacje o rachunku maksymalnie do czterech razy w ciągu 24-godzinnej okresu, o ile aktywnego żądania przekazania informacji nie składa sam klient. Ograniczenie to nie obowiązuje jednak AISP-ów posiadających umowy z dostawcami prowadzącymi rachunek (bankami), pod warunkiem, że klient wyraził zgodę.

Wynika z tego, że wbrew pozorom banki są w stanie różnicować podejście względem różnych dostawców, udostępniając części z nim informacje w systemie „ciągłym”, pozostałych zaś ograniczając w praktyce do czterech zapytań dziennie. Niemniej istotna wydaje się możliwość żądania od użytkownika SCA za każdym razem, kiedy AISP próbuje pozyskać dane o rachunku. Wprowadzenie przez bank takiego ograniczenia z pewnością zmniejszy atrakcyjność usługi oferowanej przez dany AISP, bo choć nominalnie oznacza to większe bezpieczeństwo, to w praktyce rozwiązanie tego typu będzie dla klienta dużo bardziej uciążliwe niż sytuacja, w której nie musi za każdym razem przeprowadzać procesu uwierzytelnienia.

Czy do świadczenia usług open bankingu potrzebna jest licencja?

Prosta odpowiedź na to pytanie brzmi – tak, wymagana jest albo licencja banku lub instytucji płatniczej (dla PISP/AISP) albo wpis do rejestru AISP (dla podmiotów świadczących wyłącznie usługę dostępu do informacji o rachunku).

Nie oznacza to jednak, że ww. zezwolenie musi posiadać bezpośrednio podmiot świadczący usługę końcową. Możliwe jest bowiem wystąpienie jednej z dwóch sytuacji:

- 1) usługa płatnicza (AIS lub PIS) stanowi sama w sobie część większej całości – np. uzyskiwane przez AISP z rachunku dane są wykorzystywane przez podmiot trzeci, który opierając się na nich, dokonuje analizy ryzyka (już poza samym zakresem usługi płatniczej i na podstawie wyraźnej zgody użytkownika); innym przykładem może być zastosowanie usługi inicjowania płatności (PIS) dla dokonywania opłat w sklepie internetowym; formalnie choć to dostawca licencjonowany dokonuje świadczenia usługi, to z punktu widzenia użytkownika nie stanowi on kluczowego podmiotu i relacja ta może być niemal niewidoczna;
- 2) świadczący usługę płatniczą nie posiada samodzielnego zezwolenia, działa jednak jako agent (nie należy mylić tego pojęcia z „agentem rozliczeniowym”) regulowanego TPP; oznacza to tyle, że formalnie to AISP/PISP świadczy usługę, dzieje się to jednak za pośrednictwem innego podmiotu, który w ten sposób korzysta niejako z czyjejś licencji; oczywiście nie zwalnia to TPP z odpowiedzialności za ewentualne roszczenia klientów; ponadto agent podlega wpisowi do rejestru agentów prowadzonego przez KNF, a także musi spełnić określone wymogi (np. posiadanie właściwych kompetencji przez osoby zarządzające), są one jednak znacznie mniej restrykcyjne niż te mające zastosowanie wobec licencjonowanych TPP.



STANDARDY DLA OTWARTEJ BANKOWOŚCI W EUROPIE

PSD2 oraz RTS stworzyły potrzebę wypracowania przez banki (działające jako APSP – dostawcy prowadzący rachunki, z którymi mają się łączyć TPP) jednolitych standardów specyfikacji technicznej dla interfejsów komunikacji z TPP (API). W ramach Unii Europejskiej wyróżnić można sześć największych standardów API:

1) PolishAPI (Polska)³³

Standard PolishAPI został opracowany przez Związek Banków Polskich wspólnie ze stowarzyszonymi bankami komercyjnymi i spółdzielczymi, SKOK-ami, Polską Organizacją Niebankowych Instytucji Płatności wraz ze stowarzyszonymi firmami, Polską Izbą Informatyki i Telekomunikacji, Polską Izbą Ubezpieczeń, Krajową Izbą Rozliczeniową, Biurem Informacji Kredytowej i Polskim Standardem Płatności.

Prace nad PolishAPI rozpoczęły się już w 2016 r., zaś pierwsza wersja standardu została udostępniona 17 kwietnia 2018 r. 12 grudnia 2019 r. opublikowano aktualną wersję 3.0 standardu PolishAPI. Zdecydowana większość banków działających w Polsce udostępnia API oparte na standardzie PolishAPI.

2) Berlin Group NextGenPSD2 (standard międzynarodowy)³⁴

Grupa Berlińska to paneuropejski projekt zrzeszający 26 podmiotów (w tym wymienione poniżej STET i SIBS) z krajów takich, jak Austria, Belgia, Bułgaria, Francja, Węgry, Włochy, Malta, Holandia, Portugalia, Hiszpania, Słowenia, kraje skandynawskie czy Wielka Brytania, a także działające międzynarodowo Visa i Mastercard. Grupa ta, w ramach inicjatywy Berlin Group NextGenPSD2, która zrzesza obecnie 60 różnych

³³ Więcej informacji dostępnych jest na stronie: <https://polishapi.org/>.

³⁴ Więcej informacji dostępnych jest na stronie: <https://www.berlin-group.org/psd2-access-to-bank-accounts>.

uczestników z ponad 20 krajów, przygotowała, we współpracy z kilkudziesięcioma innymi podmiotami z niemal całej Unii Europejskiej standard o tej właśnie nazwie. Pierwsza wersja standardu NextGenPSD2 została opublikowana 8 lutego 2018 r., po szerokim konsultacjach przeprowadzonych na przełomie października i listopada 2017 r., w których brało udział blisko 60 podmiotów. Obecnie, obok Polish API i Open Banking UK jest to jeden z wiodących standardów API w Europie.

3) Open Banking UK (Wielka Brytania)³⁵

W przeciwieństwie do pozostałych standardów, znajdujący zastosowanie w Wielkiej Brytanii Open Banking UK został powołany do życia przez sektor publiczny, nie jako oddolna inicjatywa uczestników rynku. Jest on prowadzony przez Open Banking Implementation Entity, które zostało założone w 2016 r. przez CMA (Competition and Markets Authority), czyli odpowiednik polskiego UOKiK (Urzędu Ochrony Konkurencji i Konsumentów). Pierwsza wersja dla tego standardu API została uruchomiona już w styczniu 2018 r.

SBAS (Słowacja)³⁷

SBA (Slovak Banking Association) rozpoczęło prace nad przygotowaniem wspólnego standardu API (SBAS) w czerwcu 2017 r., zaś wersja

Raport CMA

Jednym z motorów szybszego wprowadzenia otwartej bankowości na terenie Wielkiej Brytanii był raport CMA z 2016 r., opisujący sytuację w brytyjskim sektorze bankowości detalicznej³⁶. Zgodnie z tym raportem, podział rynku pomiędzy duże, obecne od wielu lat w sektorze banki nie sprzyjał wytworzeniu się zdrowej konkurencji pomiędzy tymi podmiotami na rynku detalicznym, co prowadziło do gorszej pozycji konsumenta i mniejszej chęci wprowadzania nowych, innowacyjnych produktów. Jednocześnie, istotne bariery wejścia powodowały, że mniejsze podmioty stykały się z problemami w zakresie nawiązania rywalizacji z dużymi bankami już istniejącymi. Te wnioski doprowadziły CMA do powołania Open Banking Implementation Entity i stworzenia zachęt do rozwoju usług otwartej bankowości na rynku brytyjskim.

1.1 standardu (już po ewaluacji przez sektor) została opublikowana w lipcu 2018 r. W ramach proponowanego przez siebie standardu SBA zrzesza 27 podmiotów, które w sumie stanowią 99% sektora słowackich banków. Jednocześnie SBAS ma charakter otwartego standardu API, którego stosowanie przez członków SBA jest całkowicie dobrowolne.

STET PSD2 (Francja)³⁸

Standard STET PSD2 został przygotowany przez STET, izbę rozliczeniową należącą do największych francuskich banków (BNP Paribas, BPCE, Crédit Agricole, Banque Fédérative du Crédit Mutuel, La Banque Postale i Société Générale). Wstępna specyfikacja została opublikowana w lipcu 2017 r., zaś dokumentacja w pełni zgodna z PSD2 i RTS ujrzała światło dzienne

w kwietniu 2018 r. Począwszy od wersji 1.3 nastąpiło zbliżenie tego standardu do dokumentacji przygotowanej przez Grupę Berlińską. Podobnie jak pozostałe wskazane standardy ma ona charakter otwartego standardu.

SIBS API Market (Portugalia)³⁹

Ostatnim z wymienionych krajowych standardów jest SIBS API Market, oferowany w Portugalii przez spółkę SIBS (Sociedade Interbancária de Serviços) powiązaną z międzybankową siecią Multibanco. Standard oferowany w ramach platformy SIBS API Market znajduje zastosowanie do połączeń z 95% wszystkich prowadzonych w Portugalii rachunków płatniczych. Podobnie jak w przypadku STET, następuje zbliżenie tego standardu do dokumentacji przygotowanej przez Grupę Berlińską.

35 Więcej informacji dostępnych jest na stronie: <https://www.openbanking.org.uk/>.

36 Pełny tekst raportu dostępny na stronie: <https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#final-report>.

37 Więcej informacji dostępnych jest na stronie: <https://sbaonline.docs.apiary.io/#> oraz (w języku słowackim) na stronie: <https://www.sbaonline.sk/projekt/slovak-banking-api-standard/>.

38 Więcej informacji dostępnych jest na stronie: <https://www.stet.eu/en/psd2/>.

39 Więcej informacji dostępnych jest na stronie: <https://www.sibsapimarket.com/>.

Dlaczego API (i ich standaryzacja) są ważne

Świadczenie usług otwartej bankowości pod PSD2 nie jest możliwe bez otwartych API. Te umożliwiają bowiem dostęp do rachunków płatniczych (z wykorzystaniem interfejsu dostępowego XS2A, od angielskiego „access to account”). W uproszczeniu pozwala on TPP na wysłanie (za uprzednią zgodą użytkownika) swego „polecenia” do dostawcy prowadzącego rachunek, który, po uwierzytelnieniu tej operacji przez użytkownika, będzie zobowiązany do przekazania informacji o rachunku do TPP albo dokonania płatności o określonych parametrach.

W celu zapewnienia lepszej jakości API, ograniczenia kosztów i ujednolicenia proponowanych rozwiązań powstały ww. standardy API, w tym PolishAPI. Brak standaryzacji API skutkowałby olbrzymimi kosztami dla sektora bankowego, każdy dostawca prowadzący rachunek musiałby bowiem w pełni samodzielnie opracowywać dokumentację API, co nie tylko zwiększałoby koszty i ryzyko błędów, ale też utrudniałoby TPP dostęp do rynku. Musiałby one każdorazowo integrować przygotowane przez siebie aplikacje z zupełnie odmiennym środowiskiem informatycznym. Dzięki jednolitym, otwartym API możliwe jest łatwiejsze i tańsze przeprowadzenie takich integracji, a dostępność, bezpieczeństwo i zgodność prawna zostają zapewnione na poziomie całego rynku. Równie ważne jest udostępnianie otwartych „sandboxów” (piaskownic), czyli wyizolowanych środowisk testowych. Pozwalają one na efektywny sposób testowania funkcjonowania projektowanych API przy jednoczesnym ograniczeniu kosztów z tym związanych, umożliwiając TPP zapoznanie się z ekosystemem technicznym jeszcze przed zainicjowaniem wdrożenia odpowiedniej usługi.

Rekomendacje PolishAPI

Ważną rolę w ramach standardów API, oprócz samej dokumentacji, mogą też pełnić rekomendacje i instrukcje w zakresie jego stosowania. Przykładem jest PolishAPI, dla którego przygotowanych zostało pięć rekomendacji. Dotykają one szczegółowych zagadnień związanych ze stosowaniem standardu i stanowią wskazówkę, w jaki sposób odnosić się do poszczególnych kwestii przez nie poruszanych. Zostały one wymienione poniżej:

1. Rekomendacje oraz podstawowe założenia do przygotowania interfejsu awaryjnego⁴⁰;
2. Rekomendacje oraz podstawowe założenia do testowania interfejsu dedykowanego⁴¹;
3. Rekomendacje dotyczące obszaru bezpieczeństwa dla podmiotów korzystających ze standardu⁴²;
4. Rekomendacja dotycząca użycia logotypów ASPSP w ramach świadczenia usług inicjacji płatności oraz dostępu do informacji o rachunku⁴³; oraz
5. Dobre praktyki UX dla usług opartych na PolishAPI⁴⁴.

⁴⁰ Dostępne na stronie: <http://docs.polishapi.org/recommendations/PolishAPI-interfejs-awaryjny-rekomendacja-v1.0.pdf>.

⁴¹ Dostępne na stronie: <http://docs.polishapi.org/recommendations/PolishAPI-testy-rekomendacja-v1.0.pdf>.

⁴² Dostępne na stronie: <https://polishapi.org/wp-content/uploads/2019/09/PolishAPI-rekomendacja-bezpieczenstwo-v1.0.pdf>.

⁴³ Dostępna na stronie: <https://polishapi.org/wp-content/uploads/2019/09/PolishAPI-rekomendacja-logotypy-v1.0.pdf>.

⁴⁴ Dostępne na stronie: <https://polishapi.org/wp-content/uploads/2020/03/DobrePraktykiUX-PolishAPI-KPMG.pdf>.



CASE STUDIES - WYBRANE MOŻLIWOŚCI WYKORZYSTANIA OTWARTEJ BANKOWOŚCI

Spośród przykładowych usług (w tym „usług premium”, wykraczających poza samą usługę płatniczą, a korzystających z możliwości oferowanych przez system otwartej bankowości m.in. w zakresie pozyskiwania informacji o rachunku) wymienić można następujące aktywności:

Usługi oparte na PIS:

- 1) Płatności, czyli inicjowanie płatności przez TPP, polegające w uproszczeniu na wydawaniu bankowi przez PISP wiążących instrukcji w zakresie dokonywania poleceń przelewu o określonych wysokościach do określonych adresatów. Usługi te być wykorzystywane zwłaszcza w branży e-commerce i płatnościach internetowych (szyb-

kie i rzetelne przelewy), w szczególności przez serwisy aukcyjne i tzw. *marketplace'y*, czyli podmioty takie, jak Allegro czy Amazon. Dzięki temu łatwo i w bezpieczny sposób można dokonywać płatności w tego typu serwisach, a ryzyko oszustw spada do minimum. Zastosowania usługi PIS są jednak dużo szersze i mogą obejmować wiele różnych modeli biznesowych opartych o dokonywanie płatności.

Przykład: Transferwise⁴⁵ umożliwia użytkownikom międzynarodowe rozliczenia bankowe w oparciu o usługę PIS, które pozwalają na często tańsze i szybsze przeprowadzanie tego rodzaju transakcji.

⁴⁵ Więcej informacji dostępnych jest na stronie: <https://api-docs.transferwise.com/#transferwise-api-payments-and-account-automation>.

Usługi oparte na AIS:

- 2) Agregowanie rachunków bankowych, już oferowane przez niektóre z banków i TPP, które polega na prowadzeniu aplikacji zbierającej dane o rachunkach klienta, także tych utrzymywanych przez różnych dostawców, w celu zaoferowania jednego, scentralizowanego interfejsu pozwalającego na łatwe śledzenie i zarządzanie wszystkimi kontami bankowymi w ramach jednej aplikacji.

Przykład: ING BS był jednym z pierwszych banków w Polsce, który umożliwił swoim klientom agregację rachunków bankowych z różnych banków w ramach jednej aplikacji⁴⁶. Innym pod-

⁴⁶ Więcej informacji dostępnych jest na stronie: <https://www.ing.pl/wiem/bankowosc-codzienna/agregator-kont-bankowych>.

miotem, dla którego agregacja rachunków (ale też inne usługi otwartej bankowości) jest kluczowa to Revolut⁴⁷, który wspólnie pracuje w tym obszarze z firmą TrueLayer⁴⁸.

- 3) Zarządzanie finansami, zarówno osobistymi, jak i biznesowymi (*personal finance management, business finance management*) oparte na analizie bieżących wydatków dokonywanych przez użytkownika rachunku płatniczego, polegające na dostarczaniu podsumowań kosztowych oraz sugestii zmian do dysponowania budżetem, w tym przy wykorzystaniu np. promocji czy okazji cenowych dla określonych kategorii produktów, z których regularnie korzysta dany klient. Ponadto duży potencjał niesie w sobie połączenie usług księgowych (biura rachunkowego) z usługą AIS, umożliwia to bowiem zautomatyzowane pobieranie danych z rachunków bankowych i w związku z tym znaczne usprawnienie dokonywania stosownych rozliczeń czy nawet świadczenia zaawansowanych usług związanych np. z rachunkowością zarządczą.

Przykład: Fincastly to polski startup wykorzystujący otwartą bankowość (a także sztuczną inteligencję) do oferowania usług związanych z tworzeniem, analizą i monitoringiem budżetu firmowego. Dzięki dostępności API

bankowych zarówno pobieranie, jak i operowanie danymi bankowymi jest dużo prostsze, a system pomaga w zarządzaniu aktywami i pasywami czy oszczędzaniu, np. poprzez informowanie o możliwości przesunięcia przychodów lub kosztów na kolejny okres rozliczeniowy.⁴⁹

- 4) Profilowanie i scoring, przy czym jest to kategoria, która może w sobie zawierać wiele rodzajów usług. Jedną z nich jest wsparcie oceny ryzyka kredytowego lub ubezpieczeniowego przy wykorzystaniu danych uzyskanych z rachunków przez TPP, co pozwala na zagregowanie i analizę przepływów na rachunku klienta i, na podstawie stosownego modelu finansowego, ocenę wpływu, jaki mogą one mieć na wiarygodność finansową takiego użytkownika. Innym przykładem może być kierowanie do klientów dedykowanych treści (np. reklam) dzięki informacjom o rachunku i dokonywanych przez klienta płatnościach, co umożliwia dostosowanie oferty handlowej dla potrzeb określonego użytkownika.

Przykład: Kontomatik dostarcza szeroką gamę usług, z których jedną z kluczowych jest ta polegająca na agregacji i analizie danych uzyskiwanych dzięki usłudze dostępu do informacji o rachunku⁵⁰. Innym przykładem jest CRIF, który również dostarcza

narzędzia (w tym te oparte na open banking) pozwalające na profilowanie klientów pod kątem ryzyka kredytowego⁵¹. Z kolei szwajcarski TASIL⁵² zwraca uwagę na to, w jaki sposób dane pozyskiwane dzięki open bankingowi mogą służyć dostosowaniu do klienta oferty reklamowej, co odgrywa szczególną rolę wśród millenialsów, będących coraz ważniejszą grupą klientów bankowych.

Usługi oparte na AIS lub PIS:

- 5) Potwierdzanie przez TPP dostępności środków lub dokonania płatności w systemach bankowych dzięki informacjom o rachunku uzyskanym od banków prowadzących rachunki dla nadawcy i adresata, co umożliwia usprawnienie zarówno informowania klienta, jak i potencjalnie przeprowadzanie rozliczeń. Usługa tego typu może też zapewniać szybsze i pewniejsze potwierdzenie dokonania transakcji (również z uwagi na niewielki margines dla możliwości cofnięcia już zleconego polecenia przelewu). Jednocześnie, dla tego typu transakcji więcej funkcjonalności prezentuje połączenie usługi AIS z usługą PIS.

Przykład: Ramp to polska spółka operująca w obszarze otwartej bankowości, blockchain i kryptoaktywów. Oferowana przez nią usługa wymiany walut cyfrowych

47 Więcej informacji dostępnych jest na stronie: <https://blog.revolut.com/open-banking-now-live-for-all-uk-customers/>.

48 Więcej informacji dostępny jest na stronie: <https://truelayer.com/customers/revolut/>.

49 Więcej informacji dostępnych jest na stronie: <https://fincastly.com/#features>.

50 Więcej informacji dostępnych jest na stronie: <https://www.kontomatik.com/products/open-banking-api/>.

51 Więcej informacji dostępnych jest na stronie: <https://docs.connector.crifrealtime.com/>.

52 Więcej informacji dostępnych jest na stronie: <https://tasil.com/insights/open-banking/>.



na pieniądź fiducyjny⁵³ opiera się na możliwości potwierdzania przez Ramp (dzięki wykorzystaniu usługi AIS i dostępowi do informacji o zrealizowanych transakcjach) wyjścia środków od kupującego i dojścia ich na rachunek sprzedawcy, co następnie w zautomatyzowany sposób transferuje sprzedawane kryptowaluty na adres kupującego widoczny na blockchainie, co umożliwia przeprowadzenie takiej wymiany w pełni *peer-to-peer* czy szeroką integrację przez podmioty wykorzystujące kryptoaktywa⁵⁴.

- 6) Potwierdzenie tożsamości i identyfikacja użytkownika w oparciu o AIS (informacjach o rachunku) lub przelewy weryfikacje, które mogą służyć zarówno wypełnieniu obowiązku przeprowadzenia wymaganej prawem od niektórych podmiotów weryfikacji dla celów AML/CFT (*anti-money laundering/counter-terrorist financing*, czyli przeciwdziałaniu praniu pieniędzy i zwalczaniu finansowania terroryzmu)⁵⁵, jak i innych rodzajów weryfikacji. Dzięki wykorzystaniu

usługi AIS możliwe jest ustalenie, że dany kontrahent w istocie posiada określone imię i nazwisko oraz prowadzi realną działalność, co daje duży potencjał zwłaszcza w obszarze wsparcia szybko rozwijającego się sektora e-commerce. Ponadto niewątpliwie klient, który posiada już rachunek bankowy, i w związku z tym został już poddany stosownym procedurom weryfikacyjnym przez bank dostawcę rachunku, jest klientem bardziej wiarygodnym.

Jednocześnie, z uwagi na już wskazane ograniczenia (brak możliwości dysponowania przez AISP-y danymi kontaktowymi czy większością danych identyfikacyjnych użytkowników), możliwość świadczenia tego typu usługi napotyka na istotne bariery. Niemniej jednak, wciąż możliwe jest potwierdzenie, że osoba o danym imieniu i nazwisku posiada określony numer rachunku bankowego oraz dokonała danych transakcji, które widoczne są w systemie bankowości elektronicznej.

Innym sposobem na weryfikację określonych informacji może być inicjacja przez PISP płatności na rzecz podmiotu, który dokonuje weryfikacji. Zgodnie bowiem z unijnym rozporządzeniem w sprawie informacji towarzyszącym transferom środków pieniężnych⁵⁶, dostawca usług

płatniczych płatnika zapewnia, by transferowi środków pieniężnych towarzyszyły określone informacje o płatniku, takie jak jego imię i nazwisko czy adres. O ile w warunkach polskich i restrykcyjnego podejścia organów wydaje się, że wciąż nie są to informacje wystarczające w odniesieniu do wymogów AML, to w innych krajach Unii Europejskiej, które dopuszczają podejście oparte na szerzej rozumianej ocenie ryzyka (*risk-based approach*) uzyskanie informacji o imieniu, nazwisku, rachunku bankowym i adresie może być wystarczające dla przeprowadzenia weryfikacji klienta.

Przykład: Nordigen to założona na Łotwie spółka, która oferuje wykorzystywanie narzędzi otwartej bankowości m.in. do wspierania procesów KYC przy wykorzystaniu informacji uzyskanych z rachunków bankowych, co w prosty sposób pozwala na zastosowanie wiarygodnego narzędzia weryfikacyjnego i ograniczenie ryzyka oszustw i wyłudzeń⁵⁷.

53 Tzw. *fiat money*, czyli środki pieniężne wyrażone w walutach krajowych, takich jak euro, dolar amerykański czy złoty.

52 Więcej informacji dostępnych jest na stronie: <https://ramp.network/>.

55 Wymogi te określa Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tekst dostępny na stronie: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000723>), która implementuje do polskiego porządku prawnego Dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającą dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającej dyrektywę 2009/138/WE i 2013/36/UE (tekst dostępny na stronie: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32018L0843>).

56 Rozporządzenie Parlamentu Europejskiego Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006 (dostępne na stronie: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32015R0847>).

57 Więcej informacji dostępnych jest na stronie: <https://nordigen.com/en/products/transaction-categorisation/>.

Wykorzystanie danych bankowych do budowania tożsamości cyfrowej

Odpowiedzią na potrzebę digitalizacji procesów gospodarczych jest idea stworzenia cyfrowej tożsamości, mogącej służyć zarówno identyfikacji uczestników obrotu gospodarczego, jak i np. zawierania przez nich umów czy weryfikacji i uwierzytelniania ich na potrzeby mechanizmów antyfraudowych (przeciwdziałania wyłudzeniom).

Interesującym przykładem zastosowania dla tego celu rozwiązań otwartej bankowości (innych niż wynikające z PSD2) jest BankID⁵⁸. Inicjatywa ta powstała w 2003 r. w Szwecji z inicjatywy największych szwedzkich banków i jest obecnie wykorzystywana przez ponad 8 milionów ludzi. BankID pozwala nie tylko na weryfikację tożsamości danej osoby, która jest potwierdzana przez bank prowadzący rachunek, ale także służy podpisywaniu umów zawieranych w sposób elektroniczny i zatwierdzaniu transakcji w obrocie gospodarczym.

W Polsce podobnym rozwiązaniem, stworzonym przez Krajową Izbę Rozliczeniową, jest usługa mojeID⁵⁹. Wśród możliwości oferowanych przez mojeID można wymienić potwierdzanie tożsamości, logowanie do istniejącego konta oraz autoryzację operacji. Usługa dostępna jest dla zweryfikowanych podmiotów (posiadających umowę z KIR), a potwierdzenie tożsamości przez użytkownika dokonywane jest poprzez logowanie się do serwisu bankowości elektronicznej. Do pewnego stopnia rozwiązania bankowe wykorzystuje w Polsce także np. profil zaufany⁶⁰, który można założyć poprzez bankowość elektroniczną, a określone czynności autoryzować za jej pomocą w sposób analogiczny do uwierzytelniania klienta na potrzeby dokonywania transakcji bankowych.

58 Więcej informacji dostępnych jest na stronie: <https://www.bankid.com/en/>.

59 Więcej informacji dostępnych jest na stronie: <https://www.mojeid.pl/#>.

60 Więcej informacji dostępnych jest na stronie: <https://www.gov.pl/web/gov/zaloz-profil-zaufany>.

POLSCY DOSTAWCY USŁUG OTWARTEJ BANKOWOŚCI



Alior Bank – agregacja kont z różnych banków przy wykorzystaniu AIS, obecnie bank oferuje w ramach usługi Alior Online podpięcia kont dla BNP Paribas Banku Polska, PKO BP, Banku Pekao, Banku Millennium, mBanku, ING Banku Śląskiego i Santander Banku Polska⁶¹; bank oferuje także uproszczony proces kredytowy, oparty na informacjach udostępnionych mu jako AISP-owi;

61 Więcej informacji dostępnych jest na stronie: <https://www.aliorbank.pl/aktualnosci/2020-07-21-alior-bank-rozwija-otwarta-bankowosc.html>.

BANKI WYKORZYSTUJĄCE ROZWIĄZANIA OTWARTEJ BANKOWOŚCI

Bank	AIS – agregacja kont	PIS – inicjowanie płatności	AIS – proces kredytowy
Alior Bank	✓		✓
ING Bank Śląski	✓		✓
mBank			✓
Bank Millennium	✓	✓	✓
PKO Bank Polski	✓		
Santander Bank Polska	✓	✓	



ING Bank Śląski – agregacja kont z różnych banków przy wykorzystaniu AIS, obecnie bank oferuje w ramach usługi Moje ING podpięcia kont dla BNP Paribas Banku Polska, PKO BP, Banku Pekao, Banku Millennium,

mBanku, Santander Banku Polska, Alior Banku i T-Mobile Usługi Bankowe⁶²; bank oferuje także uproszczony proces kredytowy, oparty na informacjach udostępnionych mu jako AISP-owi;

62 Więcej informacji dostępnych jest na stronie: <https://www.ing.pl/wiem/bankowosc-co-dzienna/open-banking>.



mBank – uproszczony proces kredytowy, oparty na informacjach o rachunku klienta w BNP Paribas Banku Polska, Banku Ochrony Środowiska, Getin Banku, PKO BP, Banku Pekao, Banku Millennium, ING Banku Śląskim, Santander Banku Polska lub Alior Banku udostępnione bankowi jako AISP-owi⁶³;



Bank Millennium – agregacja kont z różnych banków przy wykorzystaniu AIS, obecnie bank oferuje w ramach usługi Finanse 360° podpięcia kont dla BNP Paribas Banku Polska, PKO BP, Inteligo, Banku Pekao, Citi Handlowego, Banku Millennium, mBanku, ING Banku Śląskiego i Alior Banku⁶⁴; bank oferuje także uproszczony proces kredytowy, oparty na informacjach udostępnionych mu jako AISP-owi; ponadto bank daje za pośrednictwem Milletetu możliwość inicjacji płatności (usługa PIS) z kont w PKO BP, Inteligo, mBanku (z wyłączeniem przelewów pomiędzy kontami własnymi klienta), Banku Pekao, ING Banku Śląskim i Alior Banku⁶⁵;

63 Więcej informacji dostępnych jest na stronie: <https://mojebankowanie.pl/rozwiązania-otwartej-bankowosci-w-mbanku/>.

64 Więcej informacji dostępnych jest na stronie: <https://www.santander.pl/bank-porad/agregacja-kont> oraz <https://www.santander.pl/klient-indywidualny/bankowosc-interetowa/santander-open>.

65 Więcej informacji dostępnych jest na stronie: <https://www.bankmillennium.pl/bankowosc-elektroniczna/przelewy-z-innych-bankow>.



Bank Polski

PKO BP – agregacja kont z różnych banków przy wykorzystaniu AIS, obecnie bank oferuje w ramach usługi IKO podpięcia kont dla Inteligo, Santander Banku Polska, Alior Banku i T-Mobile Usługi Bankowe⁶⁶;



Santander Bank Polska – agregacja kont z różnych banków przy wykorzystaniu AIS, obecnie bank oferuje w ramach usługi Santander open podpięcia kont dla BNP Paribas Banku Polska, PKO BP, Banku Pekao, Banku Millennium, mBanku, ING Banku Śląskiego i Alior Banku⁶⁷; ponadto bank oferuje możliwość inicjacji płatności (usługa PIS) z kont w PKO BP, Banku Pekao, ING Banku Śląskim, Alior Banku i T-Mobile Usługi Bankowe.

Poza listą dostawców funkcjonuje BNP Paribas Bank Polska, który korzysta jednak w swojej działalności z rozwiązań otwartej bankowości. Wprawdzie sam nie działa on jako dostawca,

66 Więcej informacji dostępnych jest na stronie: <https://www.pkobp.pl/klienci-indywidualni/bankowosc-elektroniczna/open-banking/>.

67 Więcej informacji dostępnych jest na stronie: <https://www.santander.pl/bank-porad/agregacja-kont> oraz <https://www.santander.pl/klient-indywidualny/bankowosc-interetowa/santander-open>.

wprowadził jednak ułatwienie pozwalające klientom indywidualnym na uproszczone potwierdzenie swojej tożsamości (procedura KYC) przy przechodzeniu przez internetowy proces kredytowy. Następuje to poprzez uzyskanie przez bank dostępu do informacji o rachunku klienta posiadanym w PKO BP, Banku Pekao, Banku Millennium, mBanku, ING Banku Śląskim, Santander Banku Polska lub Alior Banku dzięki wykorzystaniu AIS⁶⁸. Jednocześnie, usługa ta działa nie w oparciu o usługę AIS świadczoną bezpośrednio przez bank, lecz przy wykorzystaniu infrastruktury dostarczanej przez spółkę Blue Media.

PODMIOTY ZNAJDUJĄCE SIĘ NA LIŚCIE DOSTAWCÓW ŚWIADCZĄCYCH USŁUGĘ DOSTĘPU DO INFORMACJI O RACHUNKU



Banqware, pod której egidą działa usługa Banqup⁶⁹, funkcjonuje jako hub dla przedsiębiorstw planujących wykorzystywać informacje pozyskiwane w ramach AIS z rachunków bankowych, zwłaszcza w modelu TPP-as-a-Service (wspierającym). W ramach proponowanego przez Banqware rozwiązania APIHub możliwe jest zbieranie i agregacja informacji o rachunku oraz wykorzystanie ich do analizy transakcji wspierającej określone modele biznesowe.

68 Więcej informacji dostępnych jest na stronie: <https://www.bnpparibas.pl/reposytoryum/komunikaty/Bank-BNP-Paribas-wykorzystuje-otwarta-bankowosc-do-potwierdzania-tozsamosci-klienta-w-nowy-sposob>.

69 Więcej informacji dostępnych jest na stronie: <https://banqup.com/>.



Kontomatik⁷⁰ to Polski AISP oferujący usługi agregacji i analizy danych podmiot oferujący bankom i instytucjom finansowym usługi w zakresie wspierania KYC i onboardingu klienta, jak również rozwiązań wspomagających procesy weryfikacyjne ocenę zdolności kredytowej. Jednocześnie Kontomatik posiada również wpis do rejestru AISP na Litwie, który spółka notyfikowała (w ramach możliwości świadczenia usługi transgranicznie) do Czech, Estonii, Francji, Niemiec, Włoch, Łotwy, Polski, Portugalii, Hiszpanii i Wielkiej Brytanii⁷¹.



Ramp⁷² wykorzystuje rozwiązania otwartej bankowości w połączeniu z unikatowymi smart contractami dla ustanowienia połączenia pomiędzy systemami bankowymi oraz blockchainem Ethereum. Dzięki temu możliwa jest łatwa integracja i rozliczanie transakcji kupna i sprzedaży kryptowalut (tj. wymiana waluty cyfrowej na pieniądź fiducyjny i w drugą stronę) bez użycia pośrednika typu custodian (tzw. atomic swaps). Pozwala to na szybkie, łatwe i bezpieczne wymiany zarówno w modelu peer-to-peer, jak i oferowanie emitentom kryptowalut i biznesom z nich korzystającym narzędzia umożliwiającego proste nabywanie aktywów cyfrowych przez klienta końcowego korzystającego z platform wykorzystywanych przez te podmioty.

70 Więcej informacji dostępnych jest na stronie: <https://www.kontomatik.com/solutions/>.

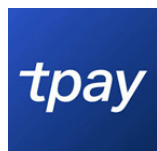
71 <https://www.lb.lt/en/sfi-financial-market-participants/kontomatik-uab>.

72 Więcej informacji dostępnych jest na stronie: <https://ramp.network/>.

KRAJOWE INSTYTUCJE PŁATNICZE (KIP) POSIADAJĄCE LICENCJĘ NA ŚWIADCZENIE USŁUG AIS I PIS

BLUE MEDIA

Blue Media⁷³ to polska spółka fintech oferująca kompleksowe rozwiązania w dziedzinie obsługi płatności internetowych oraz innych usług płatniczych. Spośród innych wymienionych w zestawieniu KIP-ów Blue Media wyróżnia fakt realnego świadczenia usług otwartej bankowości. Jak już wspomniano wyżej, Blue Media dostarcza bowiem BNP Paribas Bankowi Polska narzędzi usprawniających proces KYC na podstawie danych pozyskanych przez nią z innych rachunków bankowych klienta dzięki usłudze AIS.



Krajowy Integrator Płatności, oferujący usługę Tpay⁷⁴ wspomagającą realizację płatności online, w tym za pomocą natychmiastowych płatności typu pay-by-link. Tpay umożliwia również wykorzystanie gotowych wtyczek i modułów, pozwalających na ułatwienie wdrożenia płatności internetowych w platformach sklepowych.

73 Więcej informacji dostępnych jest na stronie: <https://bluemedia.pl/oferta>.

74 Więcej informacji dostępnych jest na stronie: <https://tpay.com/platnosci-online>.



PayPro⁷⁵ oraz **eCard**⁷⁶ (osobne instytucje płatnicze) oferują usługę Przelewy24⁷⁷ pozwalającą na dokonywanie szybkich płatności oraz inne rozwiązania płatnicze związane z zarządzaniem płatnościami oraz przyjmowaniem i rozliczaniem transakcji czy portfelami elektronicznymi.



PayU⁷⁸ to działająca od 2002 r. międzynarodowa spółka będąca operatorem płatności online, zarówno w formule kartowej, jak i za pomocą przelewu, w tym płatności za pomocą linku. Firma oferuje usługi w ponad 50 krajach w Europie, Azji, Afryce, Ameryce Południowej i Australii. Obecnym właścicielem PayU jest koncern Naspers.



Paymento Financial (tylko usługa PIS)⁷⁹ jest pochodzącym z Tychów fintechem oferującym platformy rozliczeniowe oraz rozwiązania w zakresie płatności online, kierowane głównie do instytucji finansowych oraz branży e-commerce i m-commerce. Oprócz tego spółka oferuje również terminale POS oraz integrację płatności za pomocą kryptowalut.

Należy wskazać, że to, iż jakiś podmiot znajduje się w rejestrze podmiotów mogących świadczyć określone usługi płatnicze (AIS/PIS) nie oznacza automatycznie, że takie usługi są przez



Rodzaje dostawców usług płatniczych

Największymi dostawcami usług płatniczych w Polsce są banki, które funkcjonują na podstawie ustawy prawo bankowe. Oprócz nich usługi te świadczą, działając na podstawie ustawy o usługach płatniczych, krajowe instytucje płatnicze (KIP-y), instytucje płatnicze mające siedzibę w innym państwie Unii Europejskiej (i działające w Polsce np. przez oddział albo transgranicznie – na podstawie tzw. paszportowania), a także AISP-y, czyli podmioty świadczące wyłącznie usługę dostępu do informacji o rachunku.

niego świadczone. Wielu dostawców wciąż rozwija swoje produkty, zaś część z nich, tak w Polsce, jak i za granicą, skupia się na tworzeniu połączeń z API bankowymi, umożliwiając innym biznesom na wykorzystanie rozwiązań oferowanych przez open banking w swoich usługach. Spośród wymienionych powyżej KIP-ów usługi otwartej bankowości (w tym usługę PIS) oferują Blue Media i PayU. Inne spółki w większości znajdują się obecnie na etapie opracowań produkcyjnych i technicznych bądź wdrażania poszczególnych rozwiązań do swoich modeli biznesowych.

Ustawa o usługach płatniczych wprowadza również szczególny typ dostawcy usług płatniczych, jakim jest tzw. mała instytucja płatnicza, o której mówią art. 117f–117u. Jest to rozwiązanie przeznaczone dla przedsiębiorców działających w mniejszym zakresie (miesięczna kwota transakcji nie większa niż 1 500 000 euro) lub chcących przetestować działanie swojego modelu biznesowego przed ubieganiem się o pełną licencję krajowej instytucji płatniczej. Podmiot tego typu, którym może być również osoba fizyczna, podlega wpisowi do rejestru prowadzonego przez KNF. Znajdują się w nim obecnie 62 podmioty, czyli więcej niż w rejestrze krajowych instytucji płatniczych.

Jednakże, zgodnie z przepisami ustawy, małe instytucje płatnicze mogą świadczyć usługi płatnicze inne niż AIS i PIS. Mała instytucja płatnicza nie może więc prowadzić działalności tego typu. To samo dotyczy biur usług płatniczych (inny typ podmiotu przewidziany przez ustawę), które mogą świadczyć jedynie usługę przekazu pieniężnego.

WYBRANI DOSTAWCY ŚWIADCZĄCY USŁUGI OTWARTEJ BANKOWOŚCI W UE

Spośród wielu dostawców usług otwartej bankowości w ramach Unii Europejskiej, na szczególną uwagę zasługują następujące podmioty:



Plaid⁸⁰ to wywodząca się ze Stanów Zjednoczonych spółka oferująca produkty i rozwiązania płatnicze i technologiczne zapewniające kanały dostępne do bankowych API. Spółka posiada licencję instytucji płatniczej, wydaną przez brytyjski FCA⁸¹, posiada też notyfikację pozwalającą na świadczenie działalności transgranicznej w Polsce w zakresie usługi AIS⁸².



SaltEdge⁸³ to założone w 2013 r. kanadyjsko-mołdawskie przedsiębiorstwo opierające swoją działalność na zapewnieniu TPP kanałów dostępowych, dzięki którym mogą się one łączyć z bankowymi API. Drugim filarem działalności spółki jest przygotowywanie rozwiązań technicznych dla banków

zapewniających zgodność z wymogami PSD2. SaltEdge współpracuje z ponad pięcioma tysiącami banków w 53 krajach. Spółka została zarejestrowana jako AISP przez brytyjski FCA⁸⁴, posiada też notyfikację pozwalającą na świadczenie działalności transgranicznej w Polsce w zakresie usługi AIS.



Tink⁸⁵ jest szwedzkim dostawcą świadczącym usługi otwartej bankowości. Oferuje szeroki zakres produktów, poczynsz od agregacji rachunków i inicjowania płatności, przez analitykę i edycję danych (w tym z wykorzystaniem uczenia maszynowego), po zarządzanie finansami dla gospodarstw domowych (PFM). Tink posiada status instytucji płatniczej mogącej świadczyć usługi AIS i PIS, nadany przez szwedzką Finansinspektionen⁸⁶, dysponuje także notyfikacją pozwalającą na świadczenie działalności transgranicznej w Polsce w zakresie usług AIS i PIS⁸⁷.



Token.io⁸⁸, poczynsz od 2016 r., świadczy na rzecz banków, a także innych podmiotów, usługi dostępu do API i integracji z bankami, działając zarówno jako dostawca usług płatniczych, jak i TSP. Spółka posiada

licencję instytucji płatniczej, wydaną przez brytyjski FCA⁸⁹, dysponuje także notyfikacją pozwalającą na świadczenie działalności transgranicznej w Polsce w zakresie usług AIS i PIS.



TransferWise⁹⁰ to zajmujący się płatnościami międzynarodowymi podmiot założony przez pracujących w Londynie przedsiębiorców pochodzących z Estonii. Jego aktywność koncentruje się wokół wysyłania za granicę środków pieniężnych po określonym, gwarantowanym kursie wymiany jednej waluty na drugą. Spółka posiada licencję instytucji płatniczej, wydaną przez brytyjski FCA⁹¹. O ile TransferWise dysponuje w Polsce notyfikacją w zakresie transgranicznej działalności polegającej np. na świadczeniu usług przekazu czy wydawania pieniądza elektronicznego (i realnie świadczy dla polskich klientów usługi związane z wirtualnymi portfelami czy przesyłaniem środków za granicę), to jego zezwolenie na świadczenie usług AIS i PIS nie zostało do tej pory paszportowane do Polski.



Truelayer⁹² to brytyjski dostawca oferujący połączenia z bankowymi API dla

80 Więcej informacji dostępnych jest na stronie: <https://plaid.com/eu/>.

81 Więcej informacji dostępnych jest na stronie: <https://register.fca.org.uk/s/firm?id=0010X-000049JuDPQA0>.

82 Jednocześnie, w porównaniu do innych podmiotów znajdującej się na tej liście, które najczęściej dokonały już notyfikacji w stosunku do większości krajów Unii Europejskiej, Plaid Financial dokonał tego względem jedynie 11 krajów – Danii, Finlandii, Francji, Niemiec, Irlandii, Włoch, Holandii, Norwegii, Polski, Hiszpanii i Szwecji.

83 Więcej informacji dostępnych jest na stronie: <https://www.saltedge.com/>.

84 <https://register.fca.org.uk/s/firm?id=0010X00004H79yQQAR>.

85 Więcej informacji dostępnych jest na stronie: <https://tink.com/>.

86 <https://www.fi.se/en/our-registers/company-register/details?id=145258>.

87 <https://www.fi.se/en/our-registers/company-register/gransoverskridandehandel/?id=145258>.

88 Więcej informacji dostępnych jest na stronie: <https://token.io/>.

89 Więcej informacji dostępnych jest na stronie: <https://register.fca.org.uk/s/firm?id=0010X000044E27IQAC>.

90 Więcej informacji dostępnych jest na stronie: <https://transferwise.com/pl>.

91 Więcej informacji dostępnych jest na stronie: <https://register.fca.org.uk/s/firm?id=001b000001EjC6SAAV>; TransferWise jest również wydawcą pieniądza elektronicznego i na tym opiera dużą część działalności.

92 Więcej informacji dostępnych jest na stronie: <https://truelayer.com/>.

pozyskiwania informacji o rachunku oraz inicjowania płatności. Jednym z klientów obsługiwanych przez Truelayer jest Revolut. Spółka posiada licencję instytucji płatniczej, wydaną przez brytyjski FCA⁹³, dysponuje także notyfikacją pozwalającą na świadczenie działalności transgranicznej w Polsce w zakresie usług AIS i PIS.



Yapily⁹⁴ jest spółką technologiczną dostarczającą klientom korporacyjnym platformę API umożliwiającą łączenie się z API bankowym, co pozwala na budowę aplikacji opartych na otwartej bankowości. Należąca do Yapily spółka pod nazwą Safeconnect posiada licencję instytucji płatniczej, wydaną przez brytyjski FCA⁹⁵, dysponuje też ona notyfikacją pozwalającą na świadczenie działalności transgranicznej w Polsce w zakresie usług AIS i PIS.



Yodlee⁹⁶ to powstała w 1999 r. w Stanach Zjednoczonych firma zajmująca się agregowaniem i analityką danych finansowych, dostarczająca klientom zintegrowane dane dotyczące ich operacji bankowych i inwestycji.

93 Więcej informacji dostępnych jest na stronie: <https://register.fca.org.uk/s/firm?id=001b-0000042fMZyAAM>.

94 Więcej informacji dostępnych jest na stronie: <https://www.yapily.com/>.

95 Więcej informacji dostępnych jest na stronie: <https://register.fca.org.uk/s/firm?id=0010X00004J9MH9QAN>.

96 Więcej informacji dostępnych jest na stronie <https://www.yodlee.com/europe/open-banking>.



W ramach aplikacji o nazwie money⁹⁷ firma oferuje też zaawansowane rozwiązania pozwalające zarządzać finansami domowymi (usługa PFM). Spółka została zarejestrowana jako AISP przez brytyjski FCA⁹⁸, posiada też notyfikację pozwalającą na świadczenie działalności transgranicznej w Polsce w zakresie usług AIS.

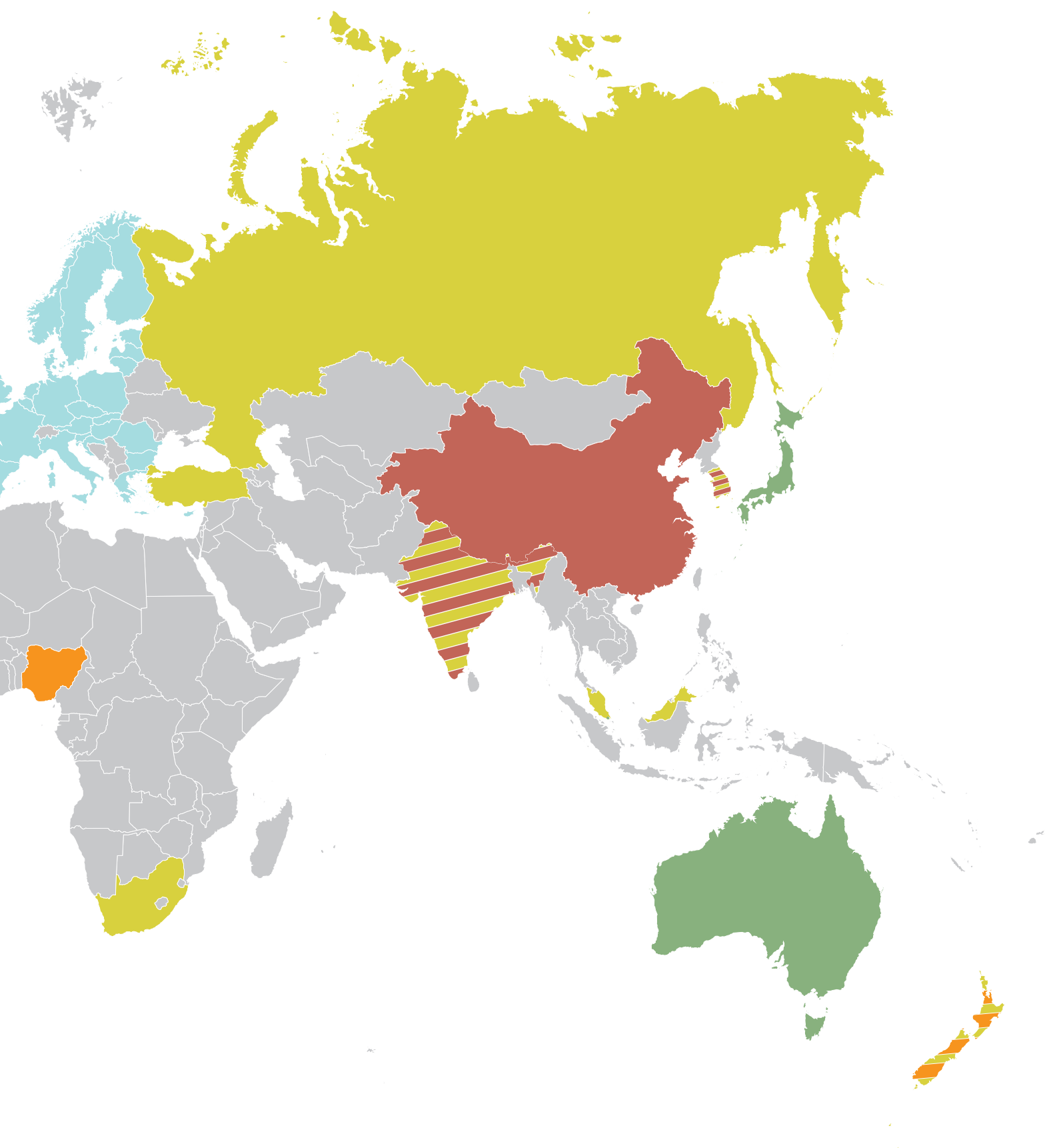
97 Więcej informacji dostępnych jest na stronie: <https://money.yodlee.com/pfm3/home>.

98 <https://register.fca.org.uk/s/firm?id=0010X-00004G2F4WQAV>.

Własne spółki świadczące usługi open banking posiadają również więksi gracze, tacy jak np. Mastercard, Revolut, Google (jako Google Payment) czy American Express. Zarówno te, jak i wymienione wyżej podmioty, mogą również świadczyć usługi płatnicze na terytorium Polski – w formie oddziału albo transgranicznie, i nie wiąże się to z koniecznością ubiegania się o odrębną licencję (wystarczające jest „notyfikowanie” już uzyskanego zezwolenia do Komisji Nadzoru Finansowego).

OPEN BANKING NA ŚWIECIE





Australia

Australia jest, oprócz Unii Europejskiej, jedną z jurysdykcji, które najszybciej wdrożyły do swojego systemu prawnego regulację otwartej bankowości. Aktem prawnym, który reguluje usługi otwartej bankowości jest Consumer Data Right (CDR)⁹⁹, który wszedł w życie 13 sierpnia 2019 r. Został on opublikowany przez Australian Competition and Consumer Commission (ACCC – australijski odpowiednik Urzędu Ochrony Konkurencji i Konsumentów), który jest jednym z inicjatorów zmian w prawie w tym zakresie oraz nadzoruje podmioty, którym przyznawane są informacje o rachunku (odpowiedniki AISP-ów).

Otwarta bankowość w Australii ma obecnie charakter ograniczony, nie obejmuje bowiem, jak dotąd, całego rynku. Począwszy od 1 lipca 2020 r., regulacja w zakresie udostępniania danych dotyczy czterech największych australijskich banków (ANZ – Australia and New Zealand Banking Group, Commonwealth Bank, NAB – National Australia Bank oraz Westpac). Przekazywane informacje mają obejmować dane transakcyjne i depozytowe oraz te powiązane z kartami debetowymi i kredytowymi, a od 1 listopada 2020 r. – także dane kredytowe, rachunki wspólne, stałe zlecenia i informacje o odbiorcy dokonywanych na rachunkach płatności. Dane te, podobnie jak przy okazji PSD2, są udostępniane jedynie podmiotom autoryzowanym (ang. Accredited Data

Recipients), które posiadają zezwolenie przyznane przez ACCC¹⁰⁰. Planuje się, aby pozostałe banki oraz ADI (Authorised Deposit-taking Institutions – inne podmioty prowadzące rachunki) zostały w pełni objęte tymi przepisami do lipca 2021 r., tak aby dać im okres przejściowy na dostosowanie się, przy czym dane o produktach podlegają udostępnianiu już od początku października 2020 r.¹⁰¹.

Interesującym faktem jest rozszerzenie regulacji australijskiej otwartej bankowości na przedsiębiorstwa spoza sektora finansowego, a konkretnie branżę energetyczną, co zostało ogłoszone 26 czerwca 2020 r.¹⁰². Przekazywane dane mają obejmować m.in. określone informacje identyfikujące klienta oraz dane o sprzedaży elektryczności (w tym oferowane produkty i zniżki), jak również dane pomiarowe, rejestrów i informacje o płatnościach.

Obecnie na liście dostawców¹⁰³ znajduje się siedem podmiotów, z czego cztery (wspomniane już banki) występują jako udostępniający dane (ang. Data Holder), pozostałe trzy zaś działają w charakterze otrzymującego dane TPP (ang. Data Recipient)¹⁰⁴.

100 Wymogi dla zostania ADR są opisane na stronie: <https://www.oaic.gov.au/consumer-data-right/cdr-participants/> oraz <https://www.cdr.gov.au/for-providers/become-accredited-data-recipient>.

101 Dokładne informacje nt. harmonogramu dostępne są na stronie: <https://www.cdr.gov.au/sites/default/files/2020-06/Revised%20phasing%20table%20-%202023%20June%202020.pdf>.

102 <https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/more-power-compare-and-switch-energy-providers>.

103 Dostępnej na stronie: <https://www.cdr.gov.au/find-a-provider>.

104 Są to: Frollo, Intuit oraz Regional Australia Bank.

Dwoma TPP spoza sektora bankowego są Frollo oraz Intuit. Frollo zapewni użytkownikom agregację posiadanych przez nich rachunków, a także dostarcza usługi z dziedziny PFM (personal finance management) w ramach dedykowanych rozwiązań technologicznych¹⁰⁵. Z kolei Intuit poprzez swoją usługę QuickBooks Online oferuje oprogramowanie i narzędzia zapewniające wsparcie w prowadzeniu księgowości¹⁰⁶. Podobnie jak Frollo, Intuit świadczy też usługi w zakresie zarządzania finansami osobistymi i korporacyjnymi.

Chiny

Chińska Republika Ludowa nie posiada regulacji open bankingowych w rozumieniu PSD2, istnieje tam jednak sformalizowana współpraca w zakresie wymiany informacji i dokonywania płatności pomiędzy największymi chińskimi bankami oraz platformami sprzedażowymi (takimi jak Alibaba) i serwisami społecznościowymi (takimi jak WeChat). Sam sektor usług e-commerce jest też w Chinach nieporównywalnie większy niż w jakimkolwiek innym kraju na świecie, co wynika nie tylko z wielkości tego rynku, ale także z przyzwyczajień konsumentów. Najbardziej popularnymi rozwiązaniami na tym rynku, które udostępniają możliwość bezpośredniego połączenia konta bankowego z ich aplikacjami, są WeChat Pay oraz AliPay¹⁰⁷.

105 Więcej informacji dostępnych jest na stronie: <https://frollo.com.au/>.

106 Więcej informacji dostępnych jest na stronie: <https://quickbooks.intuit.com/au/small-business/>.

107 Nie oznacza to jednak, że w Chinach nie ma innych firm z branży fintech, które oferują usługi płatnicze wykorzystywane przez branżę e-commerce. Przykładem jest operująca międzynarodowo firma PingPong Financial, zajmująca się głównie wsparciem obsługi płatności transgranicznych (<https://eu.pingpongx.com/eu/about>).

99 Pełny tekst przepisu oraz regulacji towarzyszących dostępny jest na stronie: <https://treasury.gov.au/consumer-data-right> oraz <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0>; wiele informacji można także znaleźć na rządowej stronie poświęconej CDR: <https://www.cdr.gov.au/>.

Należąca do koncernu Tencent (właściciela platformy społecznościowej WeChat) platforma WeChat Pay¹⁰⁸ zapewnia wbudowane w serwis społecznościowy natywne kanały płatności oparte na QR kodach i bezpośrednio rozliczenia w ramach aplikacji. WeChat Pay świadczy też usługi w zakresie płatności międzynarodowych. Model świadczenia usług transgranicznych oparty jest na bezpośredniej współpracy między grupą Tencent (właścicielem WeChat) oraz China Construction Bank i China Citic Bank¹⁰⁹.

Z kolei będąca częścią grupy Alibaba spółka fintechowa Ant Financial¹¹⁰, oprócz realizacji płatności w ramach swojego serwisu transakcyjnego, oferuje bankom i innym pożyczkodawcom zintegrowaną platformę do udzielania kredytów konsumenckich oraz pożyczek dla małych i średnich przedsiębiorstw. Operatorem płatności dla Ant Financial jest AliPay, który odpowiada za procesowanie płatności online przy wykorzystywaniu e-portfeli wbudowanych w aplikację AliPay oraz możliwość skanowania QR kodów. Podobnie jak WeChat Pay, Ant Financial posiada również zaawansowany system scoringu. Zebrane na tej podstawie dane spółka może również udostępniać innym podmiotom.

W Chinach intensywnie wykorzystuje się również informacje o kliencie dla oceny jego wiarygodności kredytowej, którą giganci technologiczni mogą następnie udostępniać bankom. Z systemu oceny zdolności kredytowej WeChat (który jest dobrowolny dla użytkowników aplikacji) korzysta już ponad 100 milionów klientów¹¹¹. Jednocześnie, z uwagi na dominację WeChat Pay oraz AliPay na rynku e-commerce, to banki są głównymi „biorcami” informacji o kliencie, co pozwala im na lepsze dokonywanie własnych ocen kredytowych. Jest to model działający w obie strony, często bowiem to dostawca w rodzaju AliPay czy WeChat Pay dysponuje większą liczbą informacji niż banki. Te bowiem, w modelu bez wymiany informacji, uzyskują jedynie wiadomość o dokonaniu przelewu na rzecz dostawcy, nie posiadają zaś danych dotyczących końcowego przeznaczenia środków, w tym do kogo realnie trafiają pieniądze.

Sztandarowym przykładem takiego mariażu jest strategiczna współpraca ICBC (Industrial and Commercial Bank of China – największy chiński bank komercyjny) oraz AliPay¹¹².

Współpraca ta, zacieśniona w pierwszej połowie 2020 r., skupia się m.in. na dostarczaniu rozwiązań technologicznych, ale zakłada też kooperację w zakresie oferowania określonych produktów bankowych. Przykładowo, firma może oferować swoim klientom produkty depozytowe (lokaty) ICBC. AliPay wychodzi zresztą

poza rynek chiński, oferując swoje usługi w kilkudziesięciu krajach na całym świecie, współpracując w tym obszarze m.in. z TransferWise.

Indie

W Indiach funkcjonuje system płatności natychmiastowych Unified Payments Interface (UPI)¹¹³ stworzony przez National Payments Corporation, pozarządową organizację zrzeszającą największe banki w kraju i podlegający regulacji banku centralnego Indii (Reserve Bank of India). Umożliwia on szybkie i uproszczone dokonywanie płatności w systemie bankowym oraz łączenie w ramach jednej aplikacji poleceń płatności dokonywanych w ramach różnych rachunków bankowych posiadanych przez jednego użytkownika. Założona w 2016 r. platforma jest obecnie wspierana przez ponad 100 banków i realizuje ponad miliard transakcji miesięcznie. UPI jest jednak inicjatywą międzybankową i trudno nazwać ją w pełni „otwartą” bankowością. W Indiach trwają też dyskusje nad wprowadzeniem nowych przepisów, które pozwoliłyby na dalszy rozwój otwartych API i systemów płatniczych.

Korea Południowa

Pierwsze kroki w kierunku stworzenia systemu otwartej bankowości Korea Południowa postawiła bardzo wcześnie, bowiem już w drugiej połowie 2016 r. pojawiły się pierwsze API dostępne, choć możliwość skorzystania z nich była ograniczona jedynie do niektórych firm. W związku z tym na początku 2019 r. koreański regulator finansowy FSC (Financial Services Commission) zaproponował

¹⁰⁸ Więcej informacji dostępnych jest na stronie: https://pay.weixin.qq.com/index.php/public/wechatpay_en.

¹⁰⁹ Więcej informacji dostępnych jest na stronie: https://pay.weixin.qq.com/wechatpay_guide/help_faq.shtml.

¹¹⁰ Więcej informacji nt. usług świadczonych przez Ant Group dostępnych jest w opublikowanych przez spółkę prospektach informacyjnych dostępnych pod następującymi adresami: <https://www1.hkexnews.hk/app/sehk/2020/102484/documents/sehk20082500535.pdf> oraz <https://www1.hkexnews.hk/listedco/listconews/sehk/2019/1115/2019111500039.pdf>.

¹¹¹ <https://www.asiatimesfinancial.com/wechat-launches-personal-credit-rating-for-600m-users>.

¹¹² Więcej informacji dostępnych jest na stronie: <https://www.alibabagroup.com/en/news/article?news=p191216>.

¹¹³ Więcej informacji dostępnych jest na stronie: <https://www.npci.org.in/product-overview/upi-product-overview>.

sektorowi wprowadzenie dalszych ułatwień dla rozwoju open bankingu, opierając się na trzech fazach: obniżenie przez banki opłat za korzystanie z systemów i dobrowolną współpracę z fintechami; wprowadzenie dedykowanych regulacji prawnych; umożliwienie autoryzowanym fintechom bezpośredniego dostępu do systemu płatniczego (bez konieczności posiadania umowy z bankiem)¹¹⁴. Jak dotąd wprowadzona została faza pierwsza, mamy więc do czynienia z oddolną inicjatywą rynkową, wspieraną przez regulatora, który dąży do ustanowienia w niedalekiej przyszłości formalnych przepisów w tym obszarze.

Obecnie w systemie otwartej bankowości uczestniczy ponad 50 firm, w tym 18 banków (pozostałe podmioty to TPP). Dostępnych jest sześć API – cztery dla usług dostępu do informacji o rachunku i dwa płatnościowe (jedna pozwalająca na pobieranie przez TPP środków z rachunku klienta, druga przeznaczona do przelewów na inne rachunki), a z usług otwartej bankowości korzysta ponad 17 milionów obywateli.

Japonia

Japońskie prawo bankowe zostało zmienione 26 maja 2017 r. w celu wprowadzenia ram dla funkcjonowania otwartych API. Regulacja ta przewiduje realizację przez TPP zarówno usług dostępu do informacji o rachunku, jak i inicjowania płatności. Sam dostęp do otwartych API jest zresztą jednym z filarów ogłoszonej przez Ministerstwo Gospodarki, Handlu i Przemysłu Japonii wizji na

rozwój sektora fintech¹¹⁵. W odróżnieniu np. od PSD2, w Japonii warunki współpracy między TPP a bankami zostały pozostawione stronom, co oznacza, że dostawcy prowadzący rachunki mogą żądać od TPP opłat za dostęp do infrastruktury bankowej. Rząd spodziewa się jednak, że do końca 2020 r. do systemu dołączy co najmniej 80 instytucji. Inne plany dotyczą też m.in. wprowadzenia cyfrowej tożsamości dla obywateli.

Hongkong

Stworzenie ram dla funkcjonowania usług otwartej bankowości w Hongkongu jest jedną z siedmiu inicjatyw dla stworzenia „inteligentnej bankowości” ogłoszonych przez Hong Kong Monetary Activity (HKMA – publiczny nadzorca bankowy w Hongkongu) we wrześniu 2017 r.¹¹⁶. Ramy dla funkcjonowania otwartego API zostały ogłoszone 18 lipca 2018 r. Do tej pory udało się wdrożyć dwie z czterech faz otwartej bankowości, czyli udostępnianie informacji o produktach oraz tych związanych z nawiązywaniem relacji z klientami (customer acquisition). Standardy techniczne dla udostępniania informacji o rachunku oraz inicjowania płatności mają zostać ogłoszone w 2020 r.

Kanada

Kanada nie posiada obecnie przepisów w zakresie otwartej bankowości. Jest jednak jednym z tych krajów, które otwarcie dyskutują na temat wprowadzenia takich regulacji. W ramach

tych dyskusji rząd zapowiedział analizę możliwości wdrożenia w Kanadzie systemu otwartej bankowości¹¹⁷, już w 2018 r. powołana też została inicjatywa Open Banking Lab. Został też wydany raport identyfikujący, jakie środki należy podjąć dla wprowadzenia open bankingu oraz możliwe formy wdrożenia rozwiązań w zakresie otwartej bankowości¹¹⁸.

Jednocześnie, ze względu na pandemię COVID-19 proces wprowadzenia w Kanadzie otwartej bankowości istotnie się opóźnia¹¹⁹ (m.in. wstrzymano z tego powodu proces przyjmowania konsultacji), co spotkało się zresztą z krytyką ze strony sektora finansowego. Podobnie jak w Stanach Zjednoczonych, zarówno banki, jak i podmioty z sektora fintech zdecydowały się na powołanie wspólnej grupy roboczej (FDX Canada Working Group)¹²⁰, w celu stworzenia wspólnych standardów i ram współpracy w obszarze otwartej bankowości. Obecnie do FDX Canada Working Group należy 31 podmiotów z sektora¹²¹.

¹¹⁷ Zostało to przewidziane w ramach budżetu na 2018 rok <https://www.budget.gc.ca/2018/docs/plan/anx-03-en.html>.

¹¹⁸ Więcej informacji dostępnych jest na stronie: <http://canada2020.ca/canada-2020-open-banking-fintech-policy-lab/>.

¹¹⁹ Doniesienia na ten temat pojawiały się m.in. tutaj: <https://betakit.com/canadas-open-banking-consultations-delayed-until-fall-at-the-earliest/>.

¹²⁰ Więcej informacji w części poświęconej Stanom Zjednoczonym, a także na stronie: <https://financialdataexchange.org/FDX/About/FDX%20Canada%20FAQ.aspx#BecomeAMember>.

¹²¹ Blanc Labs, Bank of Montreal, Capital One, CIBC, Desjardins, EEL, Envestnet | Yodlee, Equitable Bank, Finicity, FinTech Growth Syndicate (FGS), Flinks, Interac Corp., In-tuit Canada, Inverite, KOHO, Mastercard, MX, National Bank of Canada, Ninth Wave, Ozone API, Plaid, Royal Bank of Canada, SecureKey, Simplii Financial, Tangerine Bank, TD Bank Group, TrueLayer, TWG, Verify My Banks, Visa oraz Xero.

¹¹⁴ Więcej informacji dostępnych jest na stronie: https://www.fsc.go.kr/eng/new_policy/open-Banking.jsp.

¹¹⁵ Prezentacja w języku angielskim dostępna pod adresem: https://www.meti.go.jp/english/press/2017/pdf/0508_004b.pdf.

¹¹⁶ Więcej informacji dostępnych jest na stronie: <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/>.

Nigeria

W Nigerii, która nie posiada żadnej państwowej regulacji określającej ramy open banking rozwój otwartej bankowości jest wspierany przez inicjatywę Open Banking Nigeria¹²² pod egidą Open Technology Foundation. Jest to powstała w 2017 r. pozarządowa instytucja promująca otwartą bankowość. Organizacja ta, współpracując z wiodącymi podmiotami z sektora bankowego oraz fintechami, stworzyła propozycję swojego standardu API oraz zbudowała sandbox. Obecnie rozwiązanie to ma charakter propozycji zainicjowanej przez sektor, przy czym już teraz zainteresowanie nim zaczęli wyrażać międzynarodowi dostawcy, tacy jak np. TrueLayer.

Stany Zjednoczone

USA nie wprowadziło regulacji prawnych w zakresie dostępu do rachunków bankowych na wzór europejski. W odróżnieniu od niektórych innych jurysdykcji otwarta bankowość w Stanach Zjednoczonych jest głównie inicjatywą oddolną, w której istotną rolę pełni sektor bankowy. W tym celu w październiku 2018 r. powołano do życia Financial Data Exchange (FDX)¹²³, będącą częścią Financial Services Information Sharing and Analysis Center, grupę zrzeszającą uczestników sektora finansowego. Jej celem jest wypracowanie wspólnego standardu dla API oraz ram i rekomendacji pozwalających na wypracowanie systemu otwartej bankowości. W samych Stanach Zjednoczonych¹²⁴ organizacja zrzesza obecnie niemal 100 członków, w tym 24 podmioty jako „sustaining

members” oraz kolejne 75 jako „standard members”¹²⁵. FDX odpowiada także za przygotowanie swojego własnego standardu API, obecnie w wersji 4.0¹²⁶. Jak do tej pory w ramach współpracy podmiotów z sektora nie powstał jednak w pełni funkcjonalny system otwartej bankowości.

Należy też podkreślić, że pewnym utrudnieniem legislacyjnym dla przyjęcia w Stanach Zjednoczonych ogólnokrajowego systemu otwartej bankowości na podstawie inicjatywy rządowej jest dualny system prawa. Oznacza to, że oprócz regulacji federalnych, banki operujące w poszczególnych stanach mogą podlegać dodatkowym wymogom określonym w przepisach lokalnych. Nie oznacza to jednak, że amerykański legislator nie podejmował żadnych kroków w kierunku stworzenia ram prawnych dla open banking. W 2019 r. zgłoszony został też projekt ustawy pod tytułem „Open Banking Study” (H.R. 4047)¹²⁷, która nakazywałaby określonym instytucjom regulacyjnym przeprowadzenie niezależnej analizy w zakresie możliwości udostępniania danych konsumentów stronom trzecim (TPP). Nie został on jednak przyjęty. Jednocześnie, odpowiedzialna za ochronę konsumentów w sektorze finansowym agencja CFPB (Consumer Financial Protection Bureau) wydała

w październiku 2017 r. rekomendacje określające, w jaki sposób należy zapewnić ochronę praw konsumenta przekazującego dane finansowe podmiotom trzecim¹²⁸.

Pomimo braku jednolitych ram w tym zakresie Stany Zjednoczone są przykładem jurysdykcji, gdzie wiele podmiotów z rynku finansowego (i nie tylko) wykorzystuje informacje o rachunku, korzystając ze zgód klienta i wykorzystując np. screen scraping, czy inne rozwiązania oferowane przez obecnych w USA dostawców. Przykładem firmy, która w ramach swojego biznesu wykorzystuje łączenie się z rachunkami i pozyskiwanie informacji finansowych jest SoLo Funds, spółka udostępniająca platformę do pożyczek w systemie peer-to-peer¹²⁹. SoLo Funds do łączenia się z infrastrukturą bankową wykorzystało rozwiązania dostępne oferowane przez jednego z największych międzynarodowych dostawców, firmę Plaid¹³⁰.

Nowa Zelandia

Od początku w Nowej Zelandii funkcjonował model, w którym to rynek definiował kierunek, w jakim podąży otwarta bankowość. W tym celu też nowozelandzkie instytucje finansowe powołały w 2017 r. do życia Payments NZ API Centre¹³¹ jako instytucję nadzorującą stworzenie wspólnych ram organizacyjnych i standardów

¹²² Więcej informacji dostępnych jest na stronie: <https://openbanking.ng/about/>.

¹²³ Więcej informacji dostępnych jest na stronie: <https://financialdataexchange.org/>.

¹²⁴ FDX działa również w Kanadzie.

¹²⁵ Pełna lista członków dostępna jest na stronie: https://www.financialdataexchange.org/FDX/The-Consortium/Members.aspx?WebsiteKey=deae9d6d-1a7a-457b-a678-8a5517f8a474&New_ContentCollectionOrganizerCommon=2#New_ContentCollectionOrganizerCommon.

¹²⁶ Więcej informacji dostępnych jest na stronie: <https://financialdataexchange.org/FDX/News/Announcements/financial-data-exchange-releases-first-major-update-to-fdx-api-makes-fourth-version.aspx>.

¹²⁷ Tekst projektu dostępny jest na stronie: <http://www.congress.gov/116/bills/hr4047/BILLS-116hr4047ih.pdf>.

¹²⁸ Tekst rekomendacji dostępny jest na stronie: <https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/>.

¹²⁹ Więcej informacji dostępnych jest na stronie: <https://www.solofunds.com/>.

¹³⁰ Więcej informacji dostępnych jest na stronie: <https://plaid.com/customer-stories/solo/>.

¹³¹ Więcej informacji dostępnych na stronie: <https://www.apicentre.paymentsnz.co.nz/about/>.

technicznych dla open banking.

Na podstawie istniejących już teraz regulacji prawnych powstają zresztą, dzięki analizie danych bankowych, aplikacje takie, jak np. Jude¹³², która pomaga w zarządzaniu finansami domowymi.

Jednocześnie rząd Nowej Zelandii analizuje możliwość wprowadzenia aktu prawnego podobnego do australijskiego CDR¹³³. Opóźnienia we wprowadzeniu funkcjonalnego systemu open banking spotkały się też ze zniecierpliwieniem Ministerstwa Pracy, Gospodarki i Innowacji Nowej Zelandii¹³⁴. Biorąc pod uwagę ten komunikat, a także toczoną od prawie roku korespondencję z sektorem, można więc zaryzykować tezę, że punkt ciężkości we wprowadzeniu systemu otwartej bankowości w Nowej Zelandii przejdzie z poziomu porozumienia instytucji prywatnych na poziom, w którym to rząd przewodzi tej inicjatywie.

Jeśli chodzi o inne kraje, które aktywnie analizują wprowadzenie regulacji otwartej bankowości (lub wprowadziły je w jakiejś części), to można wymienić jurysdykcje takie, jak Rosja (której bank centralny dla analizy tego i innych zagadnień związanych z nowymi technologiami w finansach powołał stowarzyszenie Russian Fintech Association), Turcja, Meksyk, Japonia, RPA, Brazylia, Kolumbia czy Zjednoczone Emiraty Arabskie.

¹³² Więcej informacji dostępnych jest na stronie: <https://blog.jude.io/>.

¹³³ Oficjalny komunikat w tej sprawie: <https://www.mbie.govt.nz/business-and-employment/business/competition-regulation-and-policy/consumer-data-right/>.

¹³⁴ Korespondencja dostępna jest na stronie: <https://www.mbie.govt.nz/business-and-employment/business/competition-regulation-and-policy/consumer-data-right/retail-payment-systems-and-open-banking/>.

Oddolne inicjatywy rynkowe

Jak wspomniano powyżej, niektóre kraje zdecydowały się na odgórne stworzenie regulacji prawnych niejako „narzucających” sektorowi finansowemu współpracę w ramach ogólnodostępnych API. Z wyników przeprowadzonych wśród banków i TPP ankiety (prezentowanej poniżej) można wnioskować, że jest to rozwiązanie właściwe, bowiem oddolne inicjatywy sektora (banków i fintech), z uwagi na wielość interesariuszy, okazują się w większości być nieefektywne. Sektor sam deklaruje, że oddolne stworzenie systemu otwartej bankowości w Polsce nie byłoby zdaniem jego uczestników realistyczne. Wniosek ten potwierdza zresztą stopień zaawansowania wdrożenia rozwiązań otwartej bankowości na świecie – przodują w tym te państwa, które przyjęły powszechnie obowiązującą regulację prawną obligującą dostawców rachunków do współpracy z TPP.

Zasadniczo w krajach, które przyjęły podejście polegania na oddolnych inicjatywach sektora proces albo toczy się zdecydowanie wolniej (co może powodować interwencję ze strony regulatora, a nawet zmianę podejścia – przykładem Nowa Zelandia), albo w praktyce odbywa się on pod silnymi auspicjami instytucji centralnych (Korea Południowa, czy do pewnego stopnia Japonia).

Wyjątkiem od takiej sytuacji są Chiny, które wprowadziły nie posiadając regulacji open bankingowych, a jednak istnieją tam sformalizowane kanały komunikacji pomiędzy bankami oraz firmami technologicznymi i świadczącymi usługi płatnicze oraz prowadzącymi sprzedaż internetową, a nawet portalami społecznościowymi. Wynika to z dwóch przyczyn. Po pierwsze, stopień zaawansowania usług płatniczych świadczonych przez chińskie podmioty spoza sektora bankowego jest bardzo wysoki i można nawet powiedzieć, że w płatnościach w segmencie detalicznym to instytucje niebankowe grają rolę dominującą. Po drugie, chiński rynek jest w praktyce podzielony pomiędzy kilka dużych podmiotów. Ten brak rozdrobnienia zdecydowanie ułatwia nawiązanie porozumienia między tymi graczami, ponieważ wystarczy ustanowienie współpracy z AliPay bądź WeChat Pay dla tego, by uzyskać dostęp do istotnej części klientów. Oba powody stanowią o sukcesie modelu inicjatywy rynkowej tego quasi-open banking, gdzie wymiana informacji oraz współpraca w obszarze płatności pozwoliły na osiągnięcie sukcesu w tworzeniu tego typu rozwiązań. Jednocześnie, model chiński trudno uznać za „otwartą bankowość” w pełnym znaczeniu tego słowa, funkcjonuje on bowiem w sposób scentralizowany i oparty na kooperacji największych podmiotów. W praktyce system ten pełni jednak podobne funkcje co wykorzystywana w Europie otwarta bankowość.

WYNIKI ANKIETY

Za pośrednictwem Związku Banków Polskich do banków i TPP skierowana została ankieta, której celem była identyfikacja istniejących sentymentów rynkowych oraz ocena przez użytkowników obecnego stanu rozwoju systemu otwartej bankowości (data przeprowadzenia: sierpień–wrzesień 2020 r.). W ankiecie wzięła udział reprezentatywna grupa banków (ponad 80% ankietowanych) i TPP, przy czym część pytań skierowana była wyłącznie do banków, zaś niektórzy ankietowani nie odpowiedzieli na w niektóre pytania albo podali własne odpowiedzi. Wyniki ankiety, wraz z opisem, przedstawiamy poniżej.

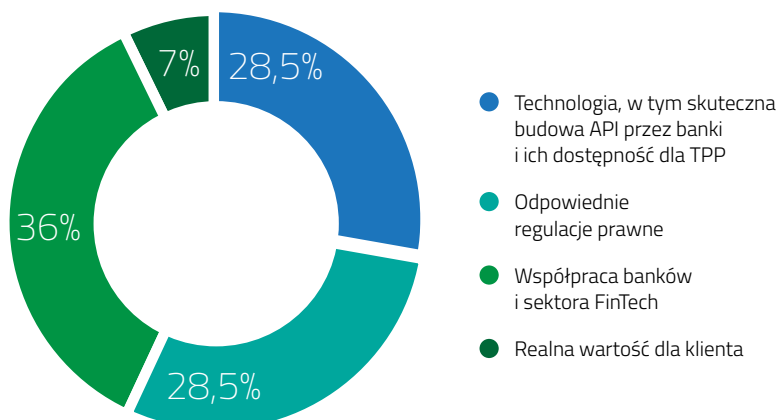
1. Który z elementów jest najważniejszy z punktu widzenia sukcesu open bankingu

Odpowiedzi na to pytanie udzielone przez podmioty poddane ankiecie są wyjątkowo zróżnicowane. Wydaje się, że każdy z zaproponowanych elementów jest istotny dla dalszego rozwoju open bankingu w Polsce. Część ankietowanych zauważa także, że banki zaczęły dostrzegać potencjał infrastruktury technicznej oferowanej przez fintechy i dlatego decydują się one na współpracę z tą branżą, wygenerowanie podobnej wartości dodanych byłoby bowiem dla banków trudniejsze lub mniej opłacane. Ankietowani wskazali także, że szczegółowe i dobrze skrojone regulacje mogą pełnić funkcję inicjatora nowych trendów i umożliwiać lepsze specyfikowanie API i określenie katalogów danych udostępnianych TPP.

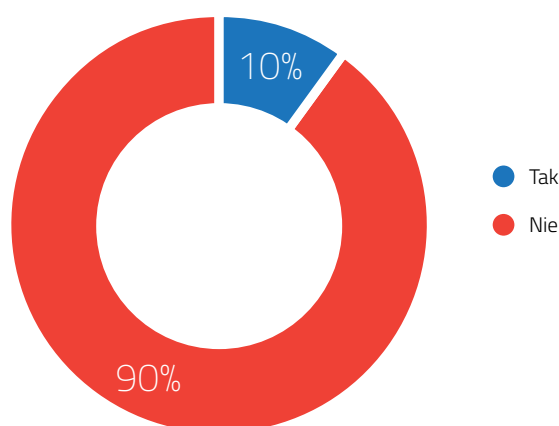
2. Czy możliwe byłoby oddolne (tj. bez interwencji regulatora) stworzenie przez sektor finansowy systemu otwartej bankowości?

Znacząca większość ankietowanych uznała, że oddolna kreacja systemu otwartej bankowości przez sektor finansowy nie byłaby możliwa. Przykład rynków działających w ramach

Najważniejsze elementy z punktu widzenia sukcesu open bankingu



Czy możliwe byłoby oddolne stworzenie przez sektor finansowy systemu otwartej bankowości?



Unii Europejskiej wskazuje, że w istocie to odgórne wprowadzenie regulacji prawnych zainicjowało system otwar-

tej bankowości, choć na świecie są też wyjątki od tej reguły (patrz część międzynarodowa).

3. Jeśli odpowiedź na pytanie nr 2 brzmi „nie”, to które z poniższych kwestii stanowiły(by) największą barierę dla stworzenia takiego systemu w przeszłości („1” to największa bariera, a „5” to najmniejsza):

Zestawienie udzielonych przez ankietowanych odpowiedzi pozwala na przypisanie poszczególnym barierom następujących uśrednionych pozycji (im niższa liczba, tym więcej ankietowanych uznało, że mamy do czynienia z bardziej istotną, w porównaniu do innych, barierą):

Brak współpracy między bankami i istnienia jednolitej inicjatywy w tym zakresie	1,67
Trudności w ujawnieniu tajemnicy bankowej	2,75
Zagrożenie nieautoryzowanych transakcji i roszczeń wobec banku	2,875
Brak potrzeby wprowadzenia z powodu już istniejących usług i form płatności (np. blik)	3,625
Niepodejmowanie inicjatyw z powodu świadomości niedługiego wprowadzenia PSD2	4

Udzielone przez ankietowanych odpowiedzi były bardzo zróżnicowane, przy czym większość podmiotów jako największy problem wskazało brak współpracy między bankami i istnienia jednolitej inicjatywy w tym zakresie – zasadniczo panował konsensus, że jest to jedna z najważniejszych przyczyn. Co do pozostałych odpowiedzi, to wskazywano je różnie – np. część podmiotów wspominała, że najważniejszym elementem była trudność w ujawnianiu tajemnicy bankowej, gdy tymczasem inne podmioty umieszczały ten problem na ostatnim miejscu.

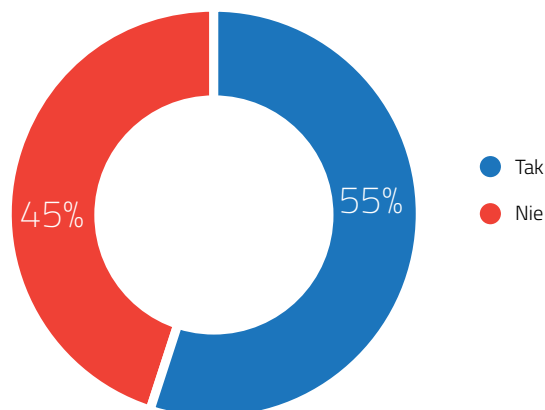
Uczestnicy ankiety, jako inne przyczyny (podawane niezależnie przez ankietowanych) wskazywali także dobrze

prosperujący rynek pośredników płatności oraz niechęć do darmowego dzielenia się danymi o rachunkach klientów, a także kwestia ryzyka regulacyjnego związanego z podjęciem takiej inicjatywy bez odgórnej regulacji UE.

4. Czy TPP, jako podmioty świadczące usługi otwartej bankowości, będą w stanie skutecznie konkurować z bankami w obszarze płatności?

Ankietowani podzielili się tutaj niemal po połowie (przy czym wszystkie TPP wskazały, że ich branża jest w stanie konkurować z bankami w obszarze płatności), z niewielką przewagą odpowiedzi „tak”. Uczestnicy ankiety wskazali tu, że ich zdaniem istnieje silna dominacja sektora bankowego, który w Polsce jest inicjatorem generacji usług otwartej bankowości. Wielu spośród ankietowanych twierdzi, że jedynie duże TPP będą miały szansę na stworzenie realnej konkurencji dla sektora bankowego. Z kolei część podmiotów jest zdania, że zasadniczo TPP i banki nie będą ze sobą konkurować, działając bowiem w innych niszach. Zwrócono też uwagę na potencjał wykorzystania TPP w branży e-commerce. Uczestnicy badania zwrócili również uwagę na fakt, że otwarta bankowość i działające w tym obszarze TPP spowodują szybszą cyfryzację i digitalizację procesów bankowych, a w rezultacie powstanie szerszy wachlarz możliwych interakcji w obszarze płatności.

Czy TPP, jako podmioty świadczące usługi otwartej bankowości, będą w stanie skutecznie konkurować z bankami w obszarze płatności?



5. Jeśli odpowiedź na pytanie nr 4 brzmi „nie”, to które z poniższych kwestii stanowiłyby główny powód, dla którego TPP nie będą mogły konkurować z bankami w tym obszarze:

1. Większe zaufanie klientów do tradycyjnych banków niż do TPP i niechęć do zmiany dostawcy
2. Ograniczenia narzucane TPP przez banki
3. Atrakcyjność innych usług oferowanych przez banki
4. TPP świadczą usługi odmiennego typu niż banki, można więc mówić o komplementarności, nie konkurencji
5. Niewielka skala działalności prowadzonej przez większość TPP

Odpowiedzi uczestników były wyjątkowo zróżnicowane (brak dominacji jednej konkretnej opcji), przy czym ankietowani wskazali w szczególności na większe zaufanie klientów do banków oraz atrakcyjność już dotychczas oferowanych usług. Banki podkreślają też, że prowadzą intensywne prace nad unowocześnianiem swojej oferty, która może stanowić dla ich klientów ciekawą alternatywę wobec TPP.

6. Czy w ciągu najbliższego roku dany podmiot zamierza świadczyć usługi otwartej bankowości inne niż polegające na prostej konsolidacji rachunków z różnych banków (usługa dostępu do informacji o rachunku)?

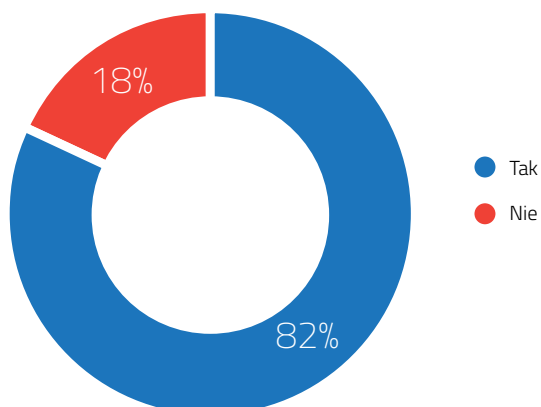
Znacząca większość ankietowanych deklaruje, że zamierza świadczyć usługi oparte na open bankingu, inne niż tylko prosta usługa konsolidacji

rachunku. Spośród tych, którzy zdecydowali się na ujawnienie usług dominowały usługi związane z inicjowaniem płatności, wykorzystujące AIS do procesu oceny zdolności kredytowej oraz procesów KYC, a także szeroko pojętego usprawniania procesów kredytowych.

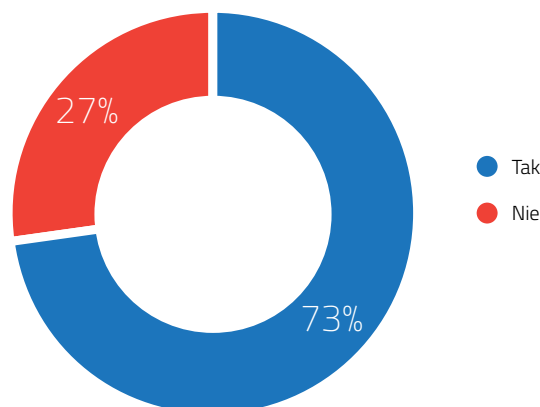
7. Czy w ciągu najbliższego roku dany podmiot zamierza wejść we współpracę z podmiotami świadczącymi usługi w branży open banking?

Ponownie, większość wskazanych podmiotów wyraziło chęć do współpracy z podmiotami z sektora fintech, a istotna część spośród nich zadeklarowała, że już z takimi podmiotami współpracuje. Spośród wskazanych typów działalności wyróżniono agregowanie danych rachunków z banków poza granicami kraju, integratory API oraz szeroko pojęte usługi związane z inicjowaniem płatności.

Czy dany podmiot planuje świadczyć w ciągu najbliższego roku usługi otwartej bankowości inne niż polegające na prostej konsolidacji rachunków z różnych banków?

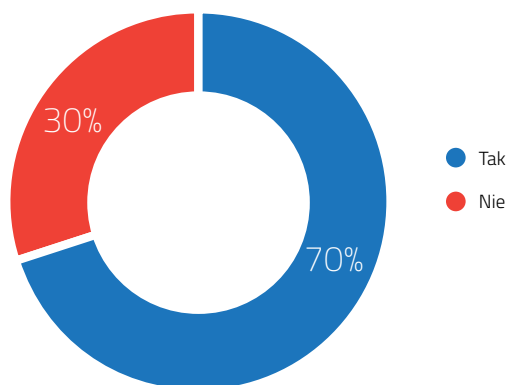


Czy w ciągu najbliższego roku dany podmiot zamierza wejść we współpracę z podmiotami świadczącymi usługi w branży open banking?



8. Czy w przypadku współpracy z TPP dany podmiot zamierza stosować dodatkowe środki bezpieczeństwa lub dozwolone prawem ograniczenia?

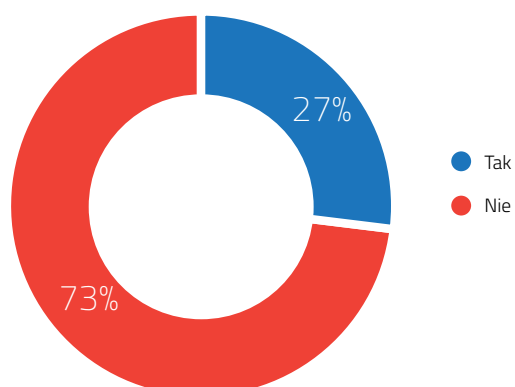
Czy w przypadku współpracy z TPP dany podmiot zamierza stosować dodatkowe środki bezpieczeństwa lub dozwolone prawem ograniczenia?



9. Czy możliwe jest różnicowanie w traktowaniu TPP, które nie posiadają z bankiem umów lub regularnej współpracy (i w związku z tym współpraca z nimi może wiązać się z większym ryzykiem)?

Jeśli chodzi o pytania 8 i 9 to ponad 2/3 banków nie zamierza stosować dodatkowych ograniczeń dla TPP poza wzmożoną komunikacją związaną z kwestią bezpieczeństwa danych. Planują one natomiast akcje informacyjne

Czy możliwe jest różnicowanie w traktowaniu TPP, które nie posiadają z bankiem umów lub regularnej współpracy?



dotyczące udostępniania danych i zjawiska phishingu. Te podmioty, które decydują się na wprowadzenie różnicowania zamierzają stosować to względem podmiotów świadczących usługi premium, które dzięki umowom zawieranim z bankami będą mogły liczyć na dodatkowe korzyści we współpracy z nimi. Niemal wszystkie banki, które zadeklarowały chęć stosowania dodatkowych mechanizmów bezpieczeństwa zamierzają różnicować podejście względem TPP, które nie posiadają zawartych z nimi umów (RTS-y dają bankom możliwość traktowania podmiotów, z którymi posiadają zawarte umowy, na uprzywilejowanych warunkach np. w zakresie częstotliwości dostępu do informacji o rachunku).

10. Jak oceniana jest inicjatywa otwartej bankowości w kształcie, jaki przyjęła pod PSD2

Liczba
głosów

Proces dostosowania się tak sektora, jak i klientów, do otwartej bankowości będzie przebiegał jako ewolucja, nie rewolucja, przy czym nie wpłynie ona znacząco na zmianę perspektywy ani upodobania klientów, przynajmniej w krótkim (kilkuletnim) horyzoncie czasowym

71%

Otwarta bankowość stanowi prawdziwą rewolucję w dziedzinie usług finansowych i z pewnością trwale zmieni to, w jaki sposób funkcjonuje ten ekosystem, potencjalnie również w obszarze występujących na nim graczy, dając większe możliwości rywalizacji firmom technologicznym

14,5%

Inne **14,5%**

Otwarta bankowość w praktyce zmieni niewiele, bo klienci nie są obecnie zainteresowani tymi usługami, a na dodatek konieczność dostosowania się do regulacji PSD2 w tym zakresie pochłonęła większość budżetu banków na innowacje

0%

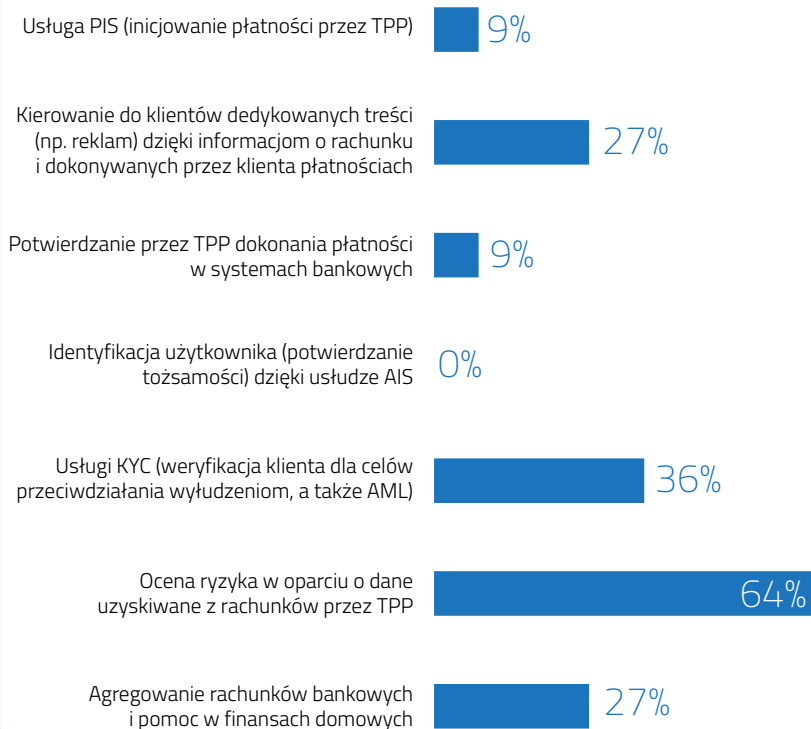
Wśród ankietowanych panowała duża zgodność w wyborze wariantu ewolucyjnego. Część spośród TPP wskazała jednak na element „rewolucyjny” i trwałą zmianę ekosystemu – różnica w ocenie open banking przez banki i TPP. Pojawiły się jednocześnie opinie, że usługi otwartej bankowości są na razie realizowane na niewielką skalę, a jako hamulcowy wskazano brak niezakłóconego działania przez API. W ocenie sektora ewolucyjny rozwój open banking może pozytywnie wpłynąć na końcową jakość, którą otrzymają użytkownicy.

11. Która z poniższych usług otwartej bankowości jest najbardziej przyszłościowa i może być na nią największy popyt?

Najczęściej wskazywaną przez ankietowanych odpowiedzią jest analiza ryzyka kredytowego, możliwa dzięki usłudze AIS, którą wskazało niemal 2/3 ankietowanych. Inne przyszłościowe usługi zdaniem podmiotów, wśród których przeprowadzono ankietę, to wykorzystanie AIS dla przeprowadzania KYC czy możliwość skorzystania z danych o rachunku do przekazywania dedykowanych treści dla klientów.

Usługi wspierające procesy kredytowe są nie tylko pożądaną przez instytucje udzielające kredytów i pożyczek ze

Najbardziej przyszłościowa usługa otwartej bankowości



względu na zmniejszenie ryzyka operacyjnego, ale także dają widoczną korzyść użytkownikom końcowym, którzy o takie pożyczki się ubiegają, ponieważ pozwalają one przyspieszyć cały proces. Proces scoringu wykorzystujący dane z rachunków bankowych może zresztą dotyczyć nie tylko oceny zdolności kredytowej, ale być przydatny także dla np. ubezpieczycieli. Obopólne korzyści płynące z tych roz-

wiązań mogą pozytywnie wpłynąć na ich komercjalizację. Ponadto uczestnicy badania zaznaczyli, że usługi PIS znacząco poszerzają możliwości banków, przyczyniając się do integracji i zwiększając stopień personalizacji usług finansowych dla konsumentów i przedsiębiorców. Podobnie jak przy poprzednich pytaniach, podkreślony został potencjał rozwiązań PIS-owych dla branży e-commerce.

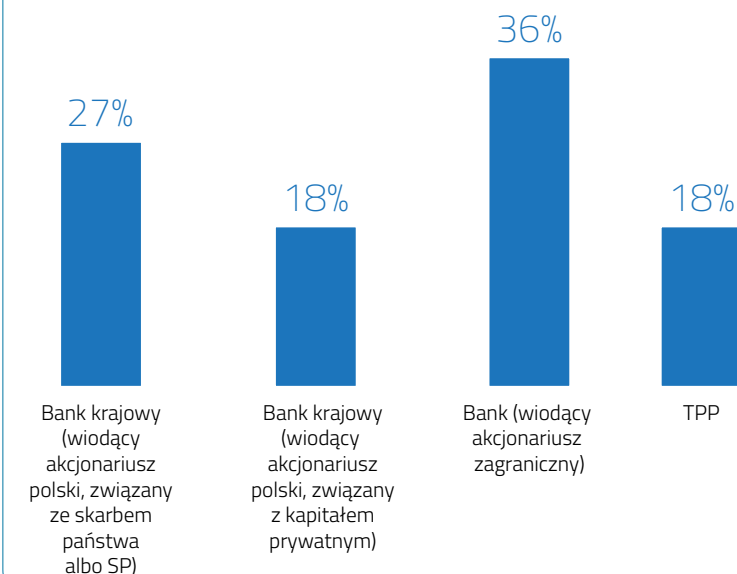


12. Typy, do których należą podmioty biorące udział w badaniu

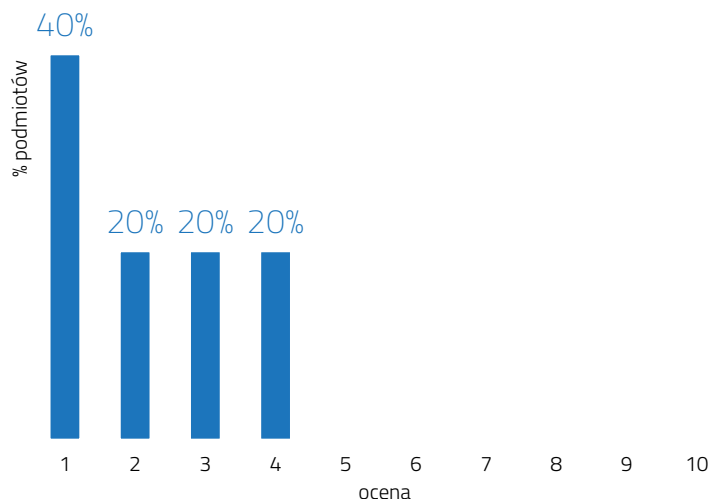
13. Dla podmiotów posiadających powiązania z kapitałem zagranicznym – jak duży był udział wiodącego podmiotu zagranicznego w ukształtowaniu podejścia do otwartej bankowości (1 – bardzo niewielki udział i duża autonomia jednostki krajowej; 10 – standardy i polityka wewnętrzna całkowicie narzucone przez podmiot dominujący)

Wszystkie podmioty, do których skierowane było pytanie, wybierały odpowiedzi z dołu skali, co świadczy o dużej swobodzie jednostek krajowych w strategicznym ujmowaniu podejścia do PSD2 i open banking.

Typy podmiotów



Udział wiodącego podmiotu zagranicznego w ukształtowaniu podejścia do otwartej bankowości



ZAKOŃCZENIE

Wydaje się, że jedną z największych zmian, jakie zaszły w ciągu ostatniego roku, jest zmiana postrzegania otwartej bankowości. O ile początkowo wśród banków w stosunku do open banking dominowało myślenie „regulacyjne”, tj. traktowanie otwartej bankowości przede wszystkim jako pewnego wyzwania prawnotechnicznego, do którego trzeba się dostosować, to obecnie obserwuje się przyjęcie podejścia produktowego. Banki zaczynają coraz bardziej dostrzegać korzyści, jakie mogą wynikać ze współpracy z branżą fintech i oferowania usług nowego typu. Widać to zarówno w odniesieniu do składanych przez sektor deklaracji, jak i zmianie oferty banków, które coraz powszechniej oferują np. integratory rachunków płatniczych.

Jednocześnie, sam rynek usług open banking nie rozwija się aż tak szybko, jak zakładali niektórzy optymiści. Możliwe jest wskazanie następujących przyczyn, dla których otwarta bankowość nie rozwija się w Polsce szybciej, a nowe usługi płatnicze mogą nie być aż tak atrakcyjne dla polskich uczestników rynku, zarówno klientów, jak i dostawców:

- 1) wysoki stopień zaawansowania stosowanych w Polsce rozwiązań płatniczych, również na tle Europy Zachodniej i Stanów Zjednoczonych;
- 2) popularność produktów już istniejących;
- 3) postępujący stopień koncentracji sektora;
- 4) brak rodzimych „challenger banków” i dużych podmiotów

typu fintech zainteresowanych budowaniem usług opartych na rozwiązaniach otwartej bankowości;

- 5) opóźnienia we wprowadzaniu przepisów umożliwiających rozpoczęcie działalności przez polskie podmioty – stosowne rozporządzenia dotyczące minimalnych sum gwarancyjnych dla AISP zostały opublikowane dopiero 31 lipca 2019 r., co w praktyce uniemożliwiało nawet złożenie wcześniej w pełni kompletnego wniosku o rejestrację AISP, nie było bowiem wiadome, w jaki sposób obliczać kwotę ubezpieczenia lub gwarancji; z kolei pierwszy wpis do rejestru AISP nastąpił dopiero pod koniec września 2019 r. (dla porównania – w Wielkiej Brytanii nastąpiło to ponad półtora roku wcześniej); jednocześnie problemy w szybkim wdrożeniu PSD2 pojawiły się nie tylko w Polsce, a wiele krajów europejskich, nawet tych, których gospodarka w dużej mierze opiera się na usługach finansowych (np. Malta), wdrożyło otwartą bankowość z jeszcze większym opóźnieniem;
- 6) wątpliwości regulacyjne;
- 7) zwiększone obciążenia regulacyjne i podatkowe (m.in. podatek bankowy), co skutkuje mniejszą ilością wolnych środków na innowacje.

Wśród zagrożeń dla dalszego rozwoju open banking wskazać też można przede wszystkim:

- ▶ niefunkcjonujące API i problemy techniczne;

- ▶ brak standaryzacji API na poziomie ogólnoeuropejskim i konieczność budowania przez TPP osobnych schematów połączeń dla każdego z banków, co jest długotrwałe i kosztowne;
- ▶ możliwe trudności we współpracy pomiędzy sektorem bankowym oraz fintechami;
- ▶ wątpliwości regulacyjne i ograniczenia prawne – np. zawężenie katalogu informacji, jakie mogą pozyskiwać AISP, co uniemożliwia w praktyce świadczenie części usług, które byłyby możliwe do wykonywania w przypadku legalności screen scrapingu; oraz
- ▶ brak zaufania klientów do usług nowego typu.

Jednym z innych pytań, jakie należy zadać, jest pytanie o przyszłość open banking, tak w Polsce, jak i w Europie oraz reszcie świata. Jeśli chodzi o to ostatnie, to z dużą dozą pewności należy założyć, że kolejne kraje będą albo wprowadzały swoje rozwiązania umożliwiające korzystanie z otwartej bankowości (najpewniej oparte na sprawdzonych regulacjach europejskich), albo tworzyły quasi-otwartą bankowość opartą na modelu chińskim, gdzie duże korporacje korzystają z możliwości pozyskiwania danych bankowych i oferowania własnych usług płatniczych. Wybór środka optymalnego dla danego środowiska prawno-ekonomicznego uzależniony jest z pewnością od struktury już istniejącego rynku i będzie zależał od wielu czynników. Z kolei zarówno w Polsce, jak i w Europie należy się spodziewać dalszego wzrostu zainteresowania usługami otwartej bankowości, tak wśród

konsumentów, których świadomość finansowa od wielu lat stale rośnie, jak i przedsiębiorstw. Te drugie mogą zyskać wiele zarówno jako klienci (wykorzystujący otwartą bankowość dla usprawnienia swojego modelu biznesowego), jak i dostawcy. Wśród oferujących te rozwiązania prym będą zapewne wiodły banki oraz wyspecjalizowane podmioty typu fintech, które w ramach proponowanych

przez siebie produktów będą w stanie zagospodarować którąś z rynkowych nisz. W najbliższych latach należy się też spodziewać dalszego zaostrzenia się już teraz zacieklej rywalizacji pomiędzy dostawcami oferującymi głównie usługi techniczne i dostępne polegające na przyłączaniu do bankowych API (bez samodzielnych usług innego typu). Trudności związane z konkurencją cenową między tymi

podmiotami, a także coraz łatwiejsze integracje mogą spowodować spadek dochodów tych firm, który jedynie w części zostanie pokryty przez wejście na rynek nowych klientów. Wzrośnie też z pewnością tendencja do korzystania z własnych rozwiązań, zamiast dostawców zewnętrznych – przynajmniej wśród podmiotów z sektora finansowego. Oznacza to zapewne, że część z dostawców skupionych na usługach dostępowych dla zachowania rentowności będzie musiała dostosować swój model biznesowy do zmieniającej się rzeczywistości i oferować coś więcej niż tylko dostęp do API. Spośród tych, którzy na tym chcą opierać swoją podstawową działalność, przetrwają najsilniejsi – ci, którzy będą oferować szeroki zakres (tj. jak najwięcej podmiotów w jak największej liczbie jurysdykcji) przyjaznych dla klienta końcowego i bezawaryjnych integracji. Rolę grać będzie także efektywny model kosztowy i cena, w jakiej oferowana jest sama usługa.

Podsumowując – można przyjąć, że wdrożenie w Polsce regulacji open banking zakończyło się sukcesem. Nie jest to może sukces spektakularny, ale mało kto zakładał, że PSD2 przyniesie rewolucję już w ciągu pierwszego roku od obowiązywania. Wręcz przeciwnie, większość ekspertów wskazywała, że zmiany na rynku będą odbywały się stopniowo – i tak też się dzieje. Ma to tę zaletę, że daje rynkowi czas na dostosowanie się do zmieniającej się rzeczywistości, a klientom na przyzwyczajenie się do usług nowego typu. Pojawili się już pierwsi dostawcy nowych usług płatniczych, a banki udostępniają API pozwalające na łączenie się z prowadzonymi przez nie w ramach bankowości elektronicznej rachunkami klientów. Sprawdzał się

W kierunku PSD3

Choć świętujemy dopiero pierwszą rocznicę wejścia w życie przepisów związanych z otwartą bankowością, już teraz pojawiają się głosy o konieczności uruchomienia prac nad kolejną odsłoną PSD – postulaty te zgłasza m.in. Emerging Payments Association w wydanym przez siebie w marcu 2020 r. raporcie¹³⁵.

Przykładowe kwestie, jakie mogłaby obejmować nowa regulacja:

- ▶ Digital ID – możliwość stworzenia cyfrowej tożsamości, która mogłaby służyć uwierzytelnianiu, ale też np. ułatwiaćby dokonanie KYC;
- ▶ pieniądź elektroniczny i tzw. waluty lokalne – jak wskazują eksperci obecna regulacja dla e-money jest dalece niewystarczająca, zaś ciesząc się popularnością „waluty lokalne” w praktyce funkcjonują w regulacyjnej próżni;
- ▶ kryptoaktywa, tokenizacja i wykorzystywanie walut cyfrowych jako środka płatniczego; oraz
- ▶ rozwiązanie wątpliwości prawnych czy poprawa niektórych mankamentów wciąż istniejących na gruncie PSD2.

Warto pamiętać, że koncepcja pt. „więcej regulacji”, nie zawsze się sprawdza, a często jest wręcz przeciwnie. Przykład PSD2 pokazuje jednak, że nowe, neutralne technologicznie przepisy mogą przysłużyć się rozwojowi nowoczesnych rozwiązań wykorzystywanych w finansach. Poruszając się w obszarze innowacji na rynku finansowym warto bowiem mieć pewność, że jest to ruch zgodny z prawem, a odpowiednie standardy i mechanizmy chroniące klienta zostały zapewnione.

¹³⁵ Raport dostępny jest na stronie: <https://www.emergingpayments.org/whitepaper/the-future-of-payments-regulation-voices-of-the-epa/>.



GAFA – nowi gracze na rynku finansowym

Wiele mówi się o możliwości wejścia dużych firm z branży technologii cyfrowych (GAFA, czyli Google, Amazon, Facebook, Apple; niektórzy dodają też do tej listy Microsoft) do sektora finansowego. Otwarta bankowość to dla tych podmiotów doskonała szansa na rozszerzenie swojej działalności właśnie o usługi płatnicze, nie muszą już bowiem tworzyć nowych, skomplikowanych rozwiązań ani budować dedykowanej infrastruktury. Wystarczy skorzystać z systemów już istniejących, do których dostęp umożliwia im właśnie open banking. Jednocześnie mogą one wykorzystać posiadane już informacje o użytkownikach i rozwiązania technologiczne do oferowania kompleksowych usług profilowanych dla indywidualnych klientów. Rozwiązań, które do niedawna kojarzyły się jeszcze jedynie z science fiction.

Jednocześnie obserwuje się już aktywne próby alternatywnego „wtargnięcia” GAFA na obszar dotychczas zarezerwowany dla banków czy instytucji płatniczych. Najlepszym przykładem jest ogłoszenie w zeszłym roku przez Facebooka planów wprowadzenia opartej na prywatnym blockchain waluty libra¹³⁶. Nie jest to zresztą pierwsza próba stworzenia nowej „waluty”, która mogłaby być wykorzystywana w płatnościach internetowych. Innymi były chociażby dobrze znany bitcoin czy powstały jeszcze pod koniec lat 90.ub.w. flooz. Jakie będą efekty działalności firm technologicznych na tym polu i czy okaże się to wielkim sukcesem, czy plajtą – pokaże czas. Jedno wydaje się pewne – trudno w dzisiejszej rzeczywistości wyobrazić sobie budowę nowego systemu płatniczego bez aktywnego udziału banków i podmiotów z sektora finansowego.

również wypracowany w ramach Związku Banków Polskich standard PolishAPI, z którego korzystają niemal wszyscy dostawcy rachunków płatniczych, a który jest rozpoznawany w Europie jako jeden z wiodących standardów dla API bankowych. Ostatnie 12 miesięcy upłynęło zarówno bankom, jak i fintechom na dostosowywaniu się do nowych regulacji oraz opracowywaniu produktów, które albo niedawno ujrzały, albo dopiero ujrzą światło dzienne. Czy kolejny rok przyniesie nowe, oparte na open bankingu rewolucyjne zmiany na rynku finansowym? Choć na to pytanie będzie można odpowiedzieć dopiero za rok, jedno wiadomo już dzisiaj – otwarta bankowość jest bliżej niż kiedykolwiek.

¹³⁶ Więcej informacji na stronie: <https://libra.org/en-US/white-paper/>.

Nowoczesne API

jako narzędzie komunikacji wewnętrznej i na zewnątrz w bankach – case studies

1 Integracja systemów globalnego banku w myśl open banking s. 79

2 Migracja usług open banking do chmury s. 81

3 Wdrażanie gotowych narzędzi open banking dostępnych na rynku s. 82

W strategii związanej z otwartą bankowością interfejsy programowania aplikacji – API – pozwalają systemom i aplikacjom bankowym komunikować się pomiędzy sobą zarówno wewnętrznie, jak i na zewnątrz. Kluczowe jest więc ich dobre zespolenie z celami biznesowymi banku. Jednym z pierwszych kroków w przygotowaniu strategii open bankingowej jest zdefiniowanie, w jaki sposób API mogą pomóc:

- ▶ W uruchomieniu nowych linii biznesowych i komercjalizacji produktów przy współpracy z zewnętrznymi dostawcami – na przykład fintechami – oraz dotarciu do wcześniej nieosiągalnych segmentów rynku;
- ▶ W udostępnieniu zasobów różnym zespołom zarówno w obrębie samego banku, jak i partnerom zewnętrznym, uniknięciu silosowości oraz kosztownych integracji end-to-end.



Szymon Kaczmarczyk

Client Unit Executive Poland & Asia Pacific,
GFT Poland

Dostosowanie do standardów otwartej bankowości to nie tylko konieczność wynikająca z wymogów regulatora, ale też szansa na rozwój nowoczesnych usług

cyfrowych, których wdrożenie było dotychczas zbyt ryzykowne kosztowo i organizacyjnie. Sytuacja, w której cały sektor bankowy podlega tym samym wymogom regulacyjnym (np. dyrektywy PSD2) wyrównuje szanse i oczekiwania. Najprostszym przykładem jest dostępność informacji o stanie kont w wielu bankach w jednej aplikacji. Swobodniejszy przepływ danych pozwala łączyć wyspy informacyjne i tworzy zupełnie nowe pole dla zdrowej konkurencji w zakresie użyteczności i przejrzystości informacji. Kluczowym czynnikiem jest w takiej sytuacji odpowiedni dobór technologii i szybki czas dostarczenia zmian lub całego rozwiązania. W tak dynamicznym i zmiennym środowisku nie ma czasu na uczenie się podczas implementacji. Zespoły GFT dokonały na przestrzeni lat wielu wdrożeń z zakresu otwartego API dla globalnych instytucji finansowych, gromadząc szeroki know-how i praktykę biznesową.

Eksperti GFT Poland



Jarosław Szczepankiewicz
Senior Solution Architect



Kamil Kłys
Technical Lead

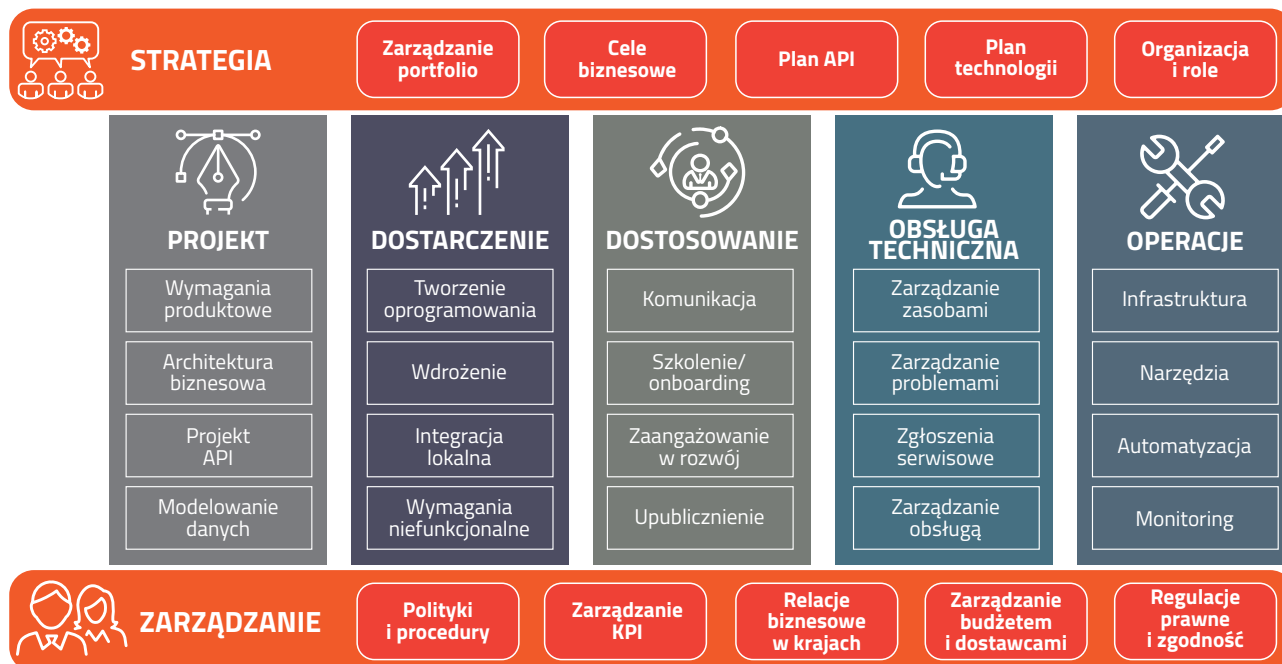


Konrad Stobiecki
Technical Lead



Piotr Mosiniak
Technical Lead

RYS. 1. Przykładowy model funkcjonalny API z funkcjami, rolami i zakresami odpowiedzialności



Aby osiągnąć te cele, należy bardzo jasno zdefiniować grupę docelową każdego API (zarówno wewnętrzną, jak i zewnętrzną), jak też portfolio usług, jakie ma udostępniać. Ze względu na skalę

działania oraz złożoność organizacyjną instytucji finansowych, należy skonsolidować ewolucję API w jedną mapę procesu, połączoną z mapą wspierających ją rozwiązań technologicznych.

Ponadto banki powinny opracować model funkcjonalny API (API capability model), który zawiera definicje funkcji, ról oraz odpowiedzialności i przedstawia je na mapie procesu. Przykładowy model przedstawiony jest na rysunku 1. W celu zagwarantowania wydajności, model funkcjonalny API musi przewidywać odpowiednio dopasowane narzędzia i technologie. Należy również podjąć szereg działań zarządczych, zapewniających zgodność API z procedurami i polityką firmy, a także regulacjami prawnymi.

Autorski framework API we współpracy z AWS

Jako zaawansowany partner AWS, rozwinęliśmy wspólny framework, który umożliwia implementację API w prosty i przystępny sposób – w ciągu zaledwie kilku tygodni. Framework ten obejmuje trzy komponenty:

- ▶ Bezserwerową architekturę (serverless), która pozwala instytucjom finansowym budować, zarządzać i udostępniać API innym organizacjom, w tym fintechom.
- ▶ Samoobsługowy sklep deweloperski (developer shop), gdzie API mogą być w prosty sposób monetizowane i udostępniane.
- ▶ Portal konsumencki, w którym deweloperzy mogą rejestrować swoje aplikacje, a konsumenci mogą korzystać z udostępnionych API.

Framework Open API opracowany przez GFT oferuje kompleksową platformę do zarządzania i udostępniania API w sposób kontrolowany, przy użyciu sprawdzonych mechanizmów, które zapewniają walidację i autoryzację użytkowników. Rozwiązanie automatycznie przechowuje całą historię transakcji w data lake, jednocześnie wspierając procesy uczenia maszynowego i analitykę. Framework oferuje najwyższy poziom bezpieczeństwa, a modele ML pozwalają aplikacjom blokować użytkowników przejawiających jakiegokolwiek anomalie w zachowaniu – wyjaśnia **Jarosław Szczepankiewicz, Senior Solution Architect GFT Poland**

CASE STUDY

INTEGRACJA SYSTEMÓW GLOBALNEGO BANKU W MYŚL OPEN BANKING

Nowoczesne bramki API

Otwarcie interfejsów programowania aplikacji (API) przynosi korzyści nie tylko w relacji z podmiotami zewnętrznymi, takimi jak regulatorzy czy innowacyjne fintechy, ale także wewnątrz samych banków. Choć

Jeden z największych banków świata wymagał integracji różnorodnych systemów wewnętrznych celem przygotowania na zmiany organizacyjne oraz dostosowania do wymogów dyrektywy PSD2. Zespół GFT opracował proces i wdrożenie, którego osią było stworzenie nowoczesnej bramki API. Wdrożona bramka pomaga zrealizować szereg celów biznesowych klienta w trzech obszarach:



1. Udostępnianie interfejsów API

- ▶ Uwspólnianie interfejsów banku pozwala udostępnić je stronom trzecim i otworzyć się na nowe funkcjonalności (mowa tu zarówno o innowacyjnych fintechach, jak i o możliwościach wynikających z dyrektyw o otwartej bankowości, takich jak PSD2).
- ▶ Wprowadzenie mechanizmów zabezpieczeń dla każdego zapytania API, w tym nadawania uprawnień firmom trzecim lub zabezpieczenia ruchu sieciowego i samych usług bankowych przed niechcianym ruchem – stosowane są standardy rynkowe, takie jak OAuth2.
- ▶ Zarządzanie dokumentacją i udostępnienie jej potencjalnym klientom (np. przez zastosowanie popularnego formatu OpenAPI Specification) – portal developerski daje dostęp do dokumentacji w formie wizualnej (HTML) oraz plików opisujących interfejsy API z wykorzystaniem OpenAPI.



2. Monitorowanie i audyt

- ▶ Monitoring wszystkich (lub wybranych) interfejsów API, w tym wykrywanie potencjalnie niebezpiecznych zachowań i operacji.
- ▶ Kontrola konsumpcji interfejsów według planów, np. przez subskrypcje konsumenckie każdego API.

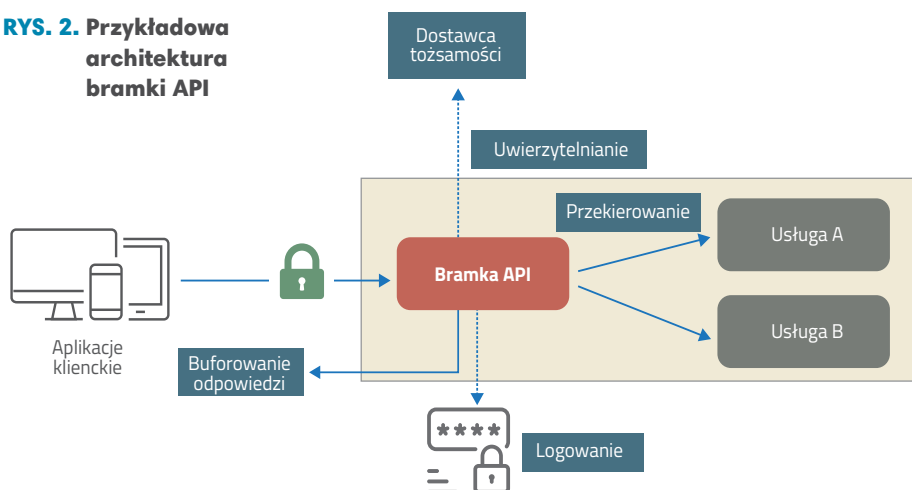


3. Transformacja cyfrowa

- ▶ Utrzymanie i rozwój nowych wersji API – wykorzystanie mechanizmu wersjonowania API, pozwalającego na równoczesne utrzymywanie oraz rozwijanie kilku wersji.
- ▶ Umożliwienie stopniowej migracji wszystkich serwisów banku na rozwiązania chmurowe – bez potrzeby wprowadzania gwałtownych zmian, zapewniając stabilne działanie usług core banking.
- ▶ Stworzenie mechanizmów zapewniających wspólną warstwę ochrony dostępu do API, dających również możliwość udostępniania całych lub częściowych interfejsów API klientom, oraz udostępnianie niekompatybilnych formatów danych (np. transformacja XML na JSON i vice versa) bez konieczności zmiany implementacji.
- ▶ Integracja z systemami banku: np. integracja bazy danych użytkowników banku z systemem API Gateway, bez konieczności ingerencji w bazę danych oraz jej interfejs.

proces ten wiąże się z dużym wysiłkiem technologicznym i organizacyjnym, otwiera przed bankami nowe możliwości w zakresie poszerzania funkcjonalności, jak i usprawnienia i unowocześnienia działania (np. ułatwiając migrację do chmury lub przejście do architektury mikroservisów, czyli procesy transformacji cyfrowej).

RYS. 2. Przykładowa architektura bramki API



– Centralnym elementem infrastruktury Open API jest bramka API (API Gateway), która pozwala oddzielić system backendowy od API udostępnionego zewnętrznie. Stanowi warstwę abstrakcji, która zapewnia dostęp do funkcjonalności banku. Innymi słowy, pozwala odizolować warstwę programistyczną, w której bank rozwija własne implementacje interfejsów API, od konsumenckiej, w której klienci lub strony trzecie korzystają z gotowych interfejsów API w sposób bezpieczny i transparentny – podkreśla **Kamil Kłys, Technical Lead, GFT Poland**.

CASE STUDY

MIGRACJA USŁUG OPEN BANKINGU DO CHMURY

Projekt dla jednego z największych banków świata oparty na Google Apigee

– Apigee jest platformą do zarządzania API firmy Google; oferuje bardzo wysoki poziom elastyczności

Klient, będący jednym z największych banków na świecie, w ramach działań z zakresu transformacji cyfrowej zwrócił się do GFT w sprawie wsparcia migracji infrastruktury do chmury Google. Zgodnie z szacunkowymi wyliczeniami, proces ten potrwa rok i obejmie większość bankowych projektów informatycznych i usług klienckich, włącznie z podstawowymi usługami wewnętrznymi, takimi jak logowanie LDAP. Połączenie technologii chmurowych Google Cloud z istniejącą infrastrukturą w banku odbywa się przy pomocy API – w synchronizacji z produktami platformy Google Apigee.

Zadanie

- ▶ Migracja usług open banking w standardzie OpenAPI do gamy produktów Apigee
- ▶ Migracja „jednym kliknięciem” API z WSO2 do Apigee
- ▶ Dostosowanie infrastruktury do istniejących usług
- ▶ Zapewnienie ciągłości usług w trakcie prac

Korzyści z wdrożenia Apigee

- ▶ Rozbudowana analityka finansowa (pobieranie danych, udostępnianie raportów)
- ▶ Lepsza ocena ryzyka (m.in. weryfikacja klienta)
- ▶ Rozbudowa wachlarza usług finansowych (zgodnie z wytycznymi PSD2 i Open Banking Working Group: uwierzytelnianie, płatności, informacje o rachunku)
- ▶ Możliwość korzystania z produktów innych instytucji finansowych

Innowacje

W rozwijającym dla klienta projekcie zastosowaliśmy m.in. następujące rozwiązania:

- ▶ **Połączenie API z istniejącym i rozwijającym od ponad roku projektem chmurowym banku, realizowanym przez hiszpański zespół GFT.** Projekt ten budowany był bez intencji połączenia go kiedykolwiek z API i udostępniania jego usług na zewnątrz, ale problem ten udało się naszemu zespołowi rozwiązać niemal natychmiast. Oznacza to, że **możemy stworzyć API do praktycznie każdego produktu, który do tej pory był przeznaczony wyłącznie do użytku wewnętrznego czy nawet offline.** Nasze rozwiązanie

można zastosować również w przypadku, gdy API serwisu, z którym chcemy się połączyć, jest niestandardowe lub przestarzałe.

- ▶ **Połączenie API z istniejącym projektem w chmurze AWS przy wykorzystaniu najnowszej technologii AWS Lambda** celem połączenia klasycznych i nowoczesnych rozwiązań IT.

- ▶ **Stworzenie logiki API opartej na danych z projektu z zerowym latencją (czasem oczekiwania na realizację połączenia sieciowego).** Zwykle bardziej rozbudowane systemy oparte na API potrzebują dodatkowych serwisów i połączeń między nimi, przez co cała infrastruktura pracuje powoli. Zaproponowane przez nas rozwiązanie pozwoliło wyeliminować ten problem. Co więcej, możemy zaimplementować API pomiędzy istniejące mikroserwisy w celu zapewnienia dodatkowej komunikacji, np. logowania, monitoringu, zabezpieczeń. **Rozwiązanie sprawia, że kod obsługujący część powiązanej z API logiki jest uruchamiany przez samo API Gateway, co redukuje konieczność tworzenia zbędnych połączeń z aplikacją i przenikania do serwisów docelowych w celu ich adaptacji do konkretnej infrastruktury.** Kultura pracy nad tworzeniem kodu, wersjonowanie, import, eksport, testing, monitoring, debugging, zostaje zachowana. Zmienia się jedynie miejsce uruchamiania kodu, co zwiększa szybkość (redukuje latencję) i bezpieczeństwo (*man in the middle*).



- ➔ **Integracja tworzenia kont użytkowników API i samych produktów API.** Naszym API da się zarządzać zarówno z konsoli panelu Apigee UI, jak i z dowolnej aplikacji, do której przywykli użytkownicy, tworzonej np. w Angular lub React. Dzięki temu nie jesteśmy ograniczeni jedynie do gotowych produktów oferowanych przez dostawcę i jednocześnie nie musimy tworzyć własnych rozwiązań do sterowania API. Możemy podłączyć istniejące frontendy platformy zarządzania do naszego API Managera.
- ▶ **Zarządzanie API za pomocą aplikacji działających na danych poza API.** API Gateway ma własną bazę danych Cassandra, jednak możemy również tworzyć logikę opartą na dowolne bazy czy usługi oraz modyfikować przesyłane dane w zależności od tego, kto i kiedy z nich korzysta i w jakim stanie są serwisy backendowe (czy działają, czy są przeciążone, czy usługi są aktywne i czy mają jakieś limity). Mogą to być bazy chmurowe – SQL jak GCP Cloud SQL, Spanner czy nierelacyjne – Bigtable, Memorystore, Firebase, Firestore. Może to być jakakolwiek inna baza czy usługa w sieci wewnętrznej, a nawet zewnętrznej, o ile latency nie jest głównym kryterium. Taką wielkoschematową aplikację podłączyliśmy do naszego API.
- ▶ **Geofencing.** Rozwiązanie jest zabezpieczone przed dostępem z nieuprawnionych krajów, np. objętych sankcjami gospodarczymi (z zerowym latency dzięki programowalnemu API).
- ▶ **Uwierzytelnienie OAuth2.** Zabezpieczenie logowania przez Industry Standard Protocol (bezpieczniejsze w porównaniu do klasycznego,

które zdradza tożsamość logującego się użytkownika).

- ▶ **Zabezpieczenie certyfikatami TLS.** Zabezpieczenie przesyłanych danych w transporcie za pomocą bezpiecznego certyfikatu.
- ▶ **Bieżący monitoring i rejestr błędów serwisów docelowych.** W technologii Apigee Hybrid połączyliśmy rozwiązania AWS i GCP z podejściem *bare metal* (klasyczna serwerownia) i dodaliśmy monitoring hybrydowego API Gateway w Graphana i Prometheus.

Oprogramowanie i usługi

Zespół GFT umożliwił wdrożenie szerokiego wachlarza rozwiązań Google:

- ▶ **Apigee Edge** – w pełni zarządzany API Gateway i API Manager.
- ▶ **Apigee Hybrid** – API Manager z wszystkimi możliwościami Apigee Edge, instalowany w dowolnym miejscu infrastruktury klienta (Anthos GKE), na dowolnej chmurze, a także on-prem.
- ▶ **Apigee Adapter for Envoy** – rozwiązanie Apigee dla proxy Envoy i service mesh, rozszerzenie Edge wewnątrz klastra Kubernetes (autoryzacja, uwierzytelnianie, limity, monitoring).
- ▶ **Cloud Endpoints** – proste API Gateway Google, które również łączy się z Apigee.
- ▶ **Google API Gateway** – beta nowego portalu Google do API (bardziej rozbudowany Endpoints, wykorzystuje OpenAPI).
- ▶ Nasze rozwiązanie API jest otwarte zarówno na istniejące, jak i nowe usługi Google Openbanking APIx.

technologicznej: działa w środowiskach chmury publicznej, prywatnej, a także w rozwiązaniach hybrydowych bądź on-premise; współpracuje też z rozwiązaniami dostawców innych niż Google Cloud Platform. Czerpiąc z ekosystemu Google, Apigee oferuje szeroki wachlarz dodatkowych funkcji, w tym zaawansowaną analitykę opartą o uczenie maszynowe – zaznacza **Konrad Stobiecki, Technical Lead, GFT Poland**.

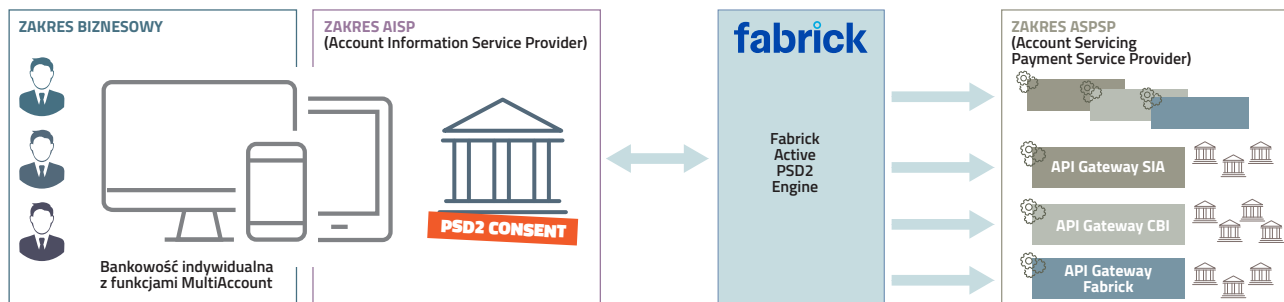
Według raportu „*Magic Quadrant for Full Life Cycle API Management*” Gartnera, Apigee znajduje się w czołówce platform do zarządzania API, m.in. z uwagi na łatwość wdrożenia i dostosowania do specyfiki klienta.

CASE STUDY

WDRAŻANIE GOTOWYCH NARZĘDZI OPEN BANKING DOSTĘPNYCH NA RYNKU

Bezpieczeństwo usług płatniczych dzięki Fabrick PSD2 Active Engine

Na rynku istnieje szereg gotowych produktów umożliwiających wdrożenie technologii open bankingowych. Jednym z nich jest PSD2 Active Engine włoskiej firmy Fabrick – platforma usług finansowych dla banków, zapewniająca takie funkcjonalności, jak agregacja kont i zarządzania różnymi rodzajami płatności.

RYS. 3. Architektura platformy Fabrick Active Engine

Zespół GFT opracował platformę frontendową dla jednego z największych włoskich banków, wykorzystującą potencjał dyrektywy PSD2. Platforma agreguje wybrane usługi wszystkich banków obecnych na rynku w ramach jednego interfejsu – dzięki czemu możliwa jest między innymi integracja kont oraz kart debetowych i kredytowych. Wdrożono mechanizm podwójnego uwierzytelnienia za pomocą tokenów OTP, powiadomień przesłanych do aplikacji lub wiadomości SMS.

– Dzięki naszemu wdrożeniu użytkownik może uzyskać dostęp do usług banku oraz wszystkich innych rachunków bankowych na określony czas. Czas dostępności usługi innego banku uzależniony jest od wymogów danego podmiotu – na ogół jest to 10 dni. By osiągnąć ten efekt, użyliśmy

rozwiązania Fabrick. Pośredniczy on w zarządzaniu zgodami usług bankowych od danego banku i odpowiedniej jej autentykacji – podkreśla **Piotr Mosiński, Technical Lead, GFT Poland**.

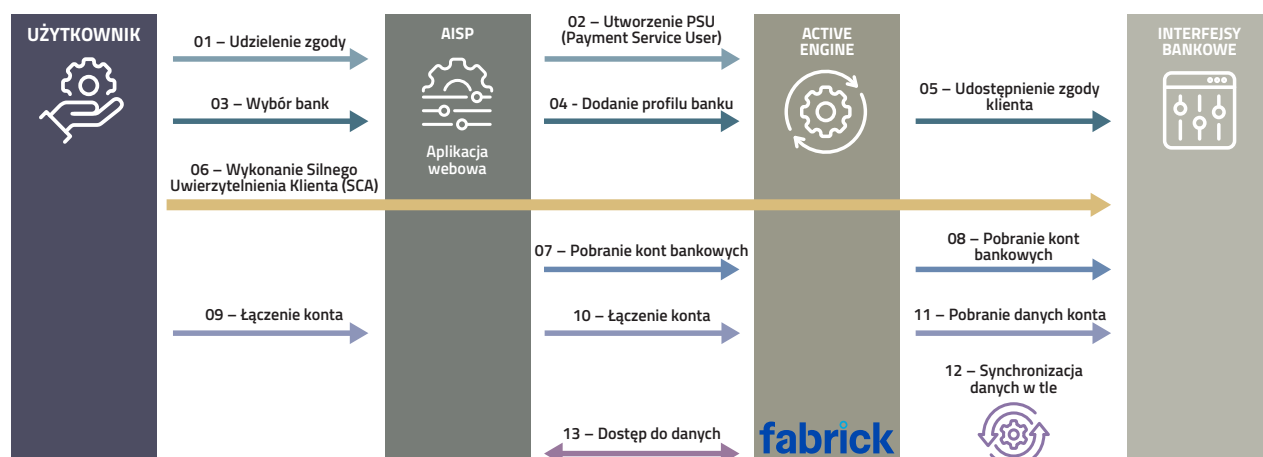
Dużym wyzwaniem było zaimplementowanie zawiłych ścieżek zgód i ich autentykacji. Dla zobrazowania skali problemu przytaczam diagram (rys. 4).

Spotykaliśmy się z czterema rodzajami zgód:

1. ALL_PSD2 – wymagana jest jedna silna autentykacja (SCA). W tym przypadku jednorazowa zgoda pozwoli użytkownikowi na dostęp do wszystkich jego rachunków i kart, w tym do związanych z nimi informacji bilansowych i przepływów.
2. BANK_OFFERED – wymagana jest jedna silna autentykacja.

W tym przypadku użytkownik usług płatniczych wybierze informacje, na które wyrazi zgodę, i które w związku z tym będzie chciał wyświetlić bezpośrednio ze strony przekierowania.

3. AVAILABLE_ACCOUNT + SPECIFIC – w tym wypadku zgoda obejmuje wyłącznie dostęp do listy rachunków i określonego produktu bankowego. Wymagana jest podwójna silna autentykacja na każdy produkt.
4. AVAILABLE_ACCOUNT + SPECIFIC_CBI – wymagana jest podwójna silna autentykacja na każdą ze zgód. Pierwszy wymaga parametru referencyjnego w ramach dostępu do treści (saldo lub transakcje), a także parametru wartości.

RYS. 4. Ścieżki zgód i uwierzytelniania

ROK BANKOWOŚCI OTWARTEJ: wygrywają tradycyjni gracze

W rocznicę wejścia w życie przepisów dyrektywy PSD2 można powiedzieć, że zapowiadana rewolucja jest raczej stopniową ewolucją, a z dostępu do „uwolnionych” danych korzystają jak na razie głównie nie fintechy, a tradycyjne banki. To one mogą zostać głównymi beneficjentami zmian i pionierami wprowadzającymi nowe rodzaje usług. Dzięki bankowości otwartej mogą też umocnić swoją pozycję przed spodziewaną ofensywą sektora GAFA. Ale najpierw muszą zbudować zaufanie nowego ekosystemu wśród swoich klientów.



■ MAŁGORZATA DOMAGAŁA

dyrektor ds. relacji
z klientem i otwartej
bankowości
Mastercard Europe

Sformułowanie „otwarta bankowość” było odmieniane przez wszystkie przypadki jeszcze zanim przepisy PSD2 weszły w życie we wrześniu 2019 r. Wielu podmiotom dają one bezprecedensowy dostęp do informacji o finansach konsumentów, tym samym dostarczając im narzędzie do zaoferowania nowych usług, optymalizacji istniejącego biznesu

lub szeroko pojętej zmiany modelu biznesowego. Bez wątpienia otwarta bankowość zmienia status quo i przynosi nowe możliwości dla wszystkich graczy z szeroko pojętego sektora finansowego.

Rewolucja odwołana?

Otwarta bankowość od początku budziła dużo emocji. Wieszczona była wielka rewolucja, zmiany niemalże tragiczne w skutkach dla banków. Fintechy, z wykorzystaniem otwartych interfejsów programistycznych (API) miały dostarczać klientom wzbogacone usługi, przejmując od banków palmę pierwszeństwa na rynku usług finansowych i sprowadzając je do roli „dawców danych”. Początkowo ekosystem nie był też do końca opisany, zrozumieli i nieznani pozostawali potencjalni nowi gracze.

Po roku od implementacji dyrektywy możemy jasno powiedzieć, że powstawanie ekosystemu otwartej bankowości jest procesem bardziej ewolucyjnym niż rewolucyjnym. Liczba banków i fintechów posiadających

licencję KNF na pobieranie informacji o stanie kont klienta w innych instytucjach rośnie stopniowo. Dziś widać przy tym jasno, że w Polsce to banki wiodą prym w obszarze otwartej bankowości. Zdecydowana większość z nich ogłosiła udostępnienie swoich produkcyjnych API tzw. podmiotom trzecim (TPP – *third party providers*). Umożliwia im to sprawdzenie funkcjonalności API i produkcyjne wdrożenie swoich usług. Z drugiej strony, banki działają również jako TPP, dzięki czemu ilość danych, do jakich zyskają dostęp, może być potencjalnie o wiele większa niż tych, które same udostępnią.

Rewolucji w bankowości niewątpliwie dokonała pandemia COVID-19. Z powodu nowych wzorców zachowań klientów wymusiła ona zmiany w sposobie funkcjonowania banków. W bardzo krótkim czasie musiały one przestawić się na cyfryzację procesów biznesowych. W wielu instytucjach plany rozwoju i roadmapy wdrożeniowe musiały zmienić się z dnia na dzień. Co jednak warto podkreślić, otwarta bankowość naturalnie



wspiera zdalne procesy bankowe (pożyczkowe, Know You Customer etc.) i jako taka może przyczynić się do szerszej rewolucji rynkowej w obszarze cyfryzacji, której jesteśmy świadkami. O ile COVID-19 może więc opóźnić niektóre wdrożenia związane z bankowością otwartą, nie jest w stanie zahamować jej rozwoju w długim terminie.

Innowacje dzięki otwartym danym

O rozwoju bankowości otwartej świadczą zmiany, które banki już wprowadziły w swojej ofercie. Są to niejednokrotnie innowacje, które mają szansę dać oferującym je instytucjom przewagę konkurencyjną.

Przepisy PSD2 pozwolą im w pełni wykorzystać potencjał nowych technologii, mogą stać się motorem innowacji, który przyspieszy wprowadzanie na rynek nowatorskich, cyfrowych rozwiązań.

Większość banków w Polsce ma ambicje stać się dostawcami takich właśnie innowacyjnych usług opartych na „uwolnionych” danych. Przykładowo Alior Bank, Bank Millennium i ING Bank Śląski już udostępniają możliwość agregacji rachunków w ramach AIS (*account information services*) w swojej aplikacji mobilnej. Zdecydowana większość sygnalizuje, że w tym kierunku również będzie zmierzać. W Banku Millennium można także zlecić przelew poprzez PSD2 (*PIS, payment initiation service*). W ten sposób banki będą na tej podstawie oferować nowe sposoby płacenia, jak również usługi oparte na informacjach z kont klientów z innych banków. Część banków deklaruje rozwój w kierunku API premium (API wykraczających poza te regulacyjne, pozwalających na pozyskanie/otrzymanie danych na warunkach komercyjnych), ale na te rozwiąza-

nia będziemy musieli jeszcze chwilę poczekać.

Banki mogą przyjąć różne strategie, aby przekuć możliwości otwartej bankowości w finansowy sukces. Mogą na przykład otworzyć się szerzej na współpracę z innymi podmiotami. Po wyrażeniu przez klienta zgody bank może wysłać do TPP informacje o potrzebach i motywacjach klientów (tzw. insighty). Te pomagają podmiotom trzecim przygotować klientom spersonalizowaną ofertę, ale za otrzymane insighty TPP przesyła bankowi wynagrodzenie.

Można też rozwinąć swoją ofertę o usługi/dane stron trzecich. Tak zrobiło kilka instytucji, np. N26, który wszedł we współpracę z kilkoma partnerami: TransferWise (płatności), Clark (ubezpieczenia), Raisin (oszczędności), Auxmoney (pożyczki), Vaamo

(wealth management). Inny przykład to aplikacja Maximum jednego z tureckich banków, wzbogacona o oferty specjalne, możliwość kupna biletów lotniczych, biletów do kina czy zamawianie jedzenia.

Z analizy rozwiązań dostępnych już na świecie wynika, że najczęstsze sposoby wykorzystania otwartej bankowości przez tradycyjne banki to możliwość wykorzystania informacji dla optymalizacji procesów pożyczkowych, analityka pod kątem x-sellu i up-sellu produktów dla klientów (sprzedaż produktów komplementarnych i sprzedaż produktów posiadanych przez klienta w innej instytucji, na korzystniejszych warunkach), rozszerzona analityka pod kątem CRM i cyklu życia klienta.

Doświadczenia z innych rynków (Europy Środkowo-Wschodniej i UE

ogólnie) pokazują, że innym ciekawym rozwiązaniem, wykraczającym poza klasyczną agregację w ramach danego kraju, jest agregacja bankowości z różnych krajów (np. z Polski i Wielkiej Brytanii) – dotyczy to zwłaszcza osób pracujących zarobkowo w innym kraju i posiadających rachunki tak w kraju pochodzenia, jak i w kraju zatrudnienia.

Nowe rodzaje usług na horyzoncie

Otwarta bankowość to szansa nie tylko na lepsze zrozumienie potrzeb klienta, ale też na zupełnie nowe rodzaje usług finansowych, które mogą zaistnieć dzięki uwolnieniu danych, dostępnych do tej pory dla jednej tylko instytucji finansowej. Z ankiet przeprowadzonych wśród klientów polskiej bankowości wynika, że takie nowinki budzą nie tylko ich ciekawość, ale też realną chęć korzystania z dodatkowych możliwości, jakie oferują. W Mastercard, na podstawie naszych doświadczeń i obserwacji z całego świata, stworzyliśmy 18 autorskich koncepcji innowacyjnych rozwiązań, które następnie zostały poddane ocenie konsumentów. Jak wynika z badania, 72% klientów banków w Polsce jest zainteresowanych tego typu nowatorskimi usługami. Ankietowanym najbardziej do gustu przypadły te z nich, które zwiększają wygodę w zarządzaniu finansami oraz gwarantują im dodatkowe korzyści, jak na przykład niższe ceny.

Przedstawione w badaniu koncepcje zostały przez ankietowanych ocenione pod kątem gotowości do skorzystania z nich, wyjątkowości i atrakcyjności. Część z tych analizowanych koncepcji usług jest możliwa do wdrożenia



bezpośrednio na podstawie dyrektywy PSD2, część wymaga działań bilateralnych w ramach API Premium. Największą szansę na rynkowy sukces wydają się mieć nowatorskie usługi, z których klienci chętnie by skorzystali:

- Zakupy warunkowe „kup, kiedy będzie taniej” – umożliwia złożenie w sklepie internetowym korzystniejszego zlecenia typu „kup, kiedy produkt będzie tańszy o X%/X PLN, a ja będę miał środki na koncie”.
- Wszystkie rachunki w jednym miejscu – pozwala na podgląd rachunków oraz historii transakcji z kilku banków w jednym miejscu.
- Ankiety tematyczne w aplikacji bankowej – dopasowane do demograficzno-zakupowego profilu klienta. Ich wypełnienie gwarantowałoby dodatkowe rabaty lub bilety do kina.
- Uproszczony proces pokalizyjny – usługa ubezpieczeniowa, która w przypadku stłuczki samochodowej prowadzi klienta przez proces likwidacji szkody.
- Zlecanie przelewów i płatności w jednym miejscu – usługa umożliwia realizację przelewów ze wszystkich podłączonych kont bankowych w jednym miejscu.
- Oferowanie produktów bankowych – bank, dzięki podłączeniu do niego rachunków z innych banków widzi, z jakich produktów korzysta tam klient i jest w stanie przedstawić ofertę na korzystniejszych warunkach.

Inne, ciekawe koncepcje usług pozytywnie ocenione przez klientów to

m.in.: zakupy warunkowe „kup, kiedy będę miał pieniądze”; telefon/internet/prąd na lepszych warunkach; zarządzanie subskrypcjami; oraz zaawansowany asystent finansowy.

„Open data” nie tylko w Unii Europejskiej

Widzimy zatem stałe, ewolucyjne zmiany na rynku, coraz szersze otwieranie się przez banki, poszukiwanie strategii „więcej niż bank”. Nowe możliwości banków warto rozpatrywać jednak nie tylko z perspektywy szerszej oferty, ale też szerszego wachlarza instytucji, z którymi mogą współpracować – zarówno pod względem geograficznym, jak i branżowym.

Perspektywę na otwartą bankowość należy rozszerzyć poza Unię Europejską. Trendy w obszarze otwierania dostępu do bankowości obserwujemy bowiem globalnie, począwszy od USA, poprzez Australię, a skończywszy na



W Polsce to banki wiodą prym w obszarze otwartej bankowości. Zdecydowana większość z nich ogłosiła udostępnienie swoich produkcyjnych API tzw. podmiotom trzecim (TPP). Umożliwia im to sprawdzenie funkcjonalności API i produkcyjne wdrożenie swoich usług. Z drugiej strony, banki działają również jako TPP, dzięki czemu ilość danych, do jakich zyskują dostęp, może być potencjalnie o wiele większa niż tych, które same udostępniają.

Hongkongu czy Singapurze. Co ciekawe, kraje europejskie pozostające poza UE (w tym nasz najbliższy sąsiad, Ukraina), także bacznie przyglądają się tematowi i są zaawansowane w działaniach mających umożliwić lokalnym graczom oferowanie rozwiązań z obszaru otwartej bankowości. W praktyce oznacza to, że ekosystem daje możliwość dostępu do ponad 9 tys. instytucji finansowych w samym Europejskim Obszarze Gospodarczym, jak również do setek tysięcy innych biznesowych partnerów na całym świecie, którzy dostrzegają możliwości, jakie ten ekosystem niesie.

Fenomen, z którym się spotykamy, nie dotyczy też wyłącznie graczy bankowych. Dlatego coraz częściej słyszymy nowy buzz word, który brzmi „open data”. Nic bowiem

nie stoi na przeszkodzie, by podobne możliwości dostępu i wymiany danych dotyczyły także firm telekomunikacyjnych, dostawców mediów, szeroko pojętego handlu itd.

Jako organizacja globalna, Mastercard przygląda się temu tematowi od początku. Wierzymy, że bankowość otwarta będzie rozwijała się w kierunku globalizacji i standaryzacji, co pozwoli na swobodny przepływ danych na całym świecie. Dlatego też stworzyliśmy całą gamę rozwiązań pod nazwą Mastercard Open Banking Solutions, z których korzystają już m.in. znane w Polsce Aion i DiPocket.

GAFA zwiera szyki

Z otwarcia dostępu do danych finansowych będą korzystać też giganci technologiczni, tacy jak Google, Apple, Facebook czy Amazon (tzw. firmy GAFA). Ich głównym

sposobem generowania przychodów jest agregowanie danych i monetizacja insightów. Mają już one gros danych o kliencie, ale brakuje im tych finansowych. To już się jednak zmienia. Google właśnie porozumiał się z ośmioma bankami, takimi jak np. BBVA, dzięki czemu będzie mógł oferować usługi finansowe na zasadzie white label, gdzie Google będzie zapewniać doświadczenie użytkownika, a formalnie klient będzie podpisywać umowę z bankiem. W ten sposób gigant z Mountain View uzyska dostęp do danych finansowych, co może być początkiem nowej rewolucji na rynku finansowym. Tutaj otwarta bankowość może przyjść tradycyjnym bankom w sukurs, pomagając im zadbać o konkurencyjność. Dobrze wykorzystana do poprawy doświadczenia użytkownika da bankom szansę na zmierzenie się z sektorem GAFA i rywalizowania z nim o lojalność klienta. Choć polskie

banki są bardziej innowacyjne niż te w krajach Europy Zachodniej, również nad Wisłą bankowcy powinni uważnie śledzić posunięcia technologicznych gigantów i starać się zająć open banking jako ich obszar kompetencyjny.

Bez zaufania klientów ani rusz

Żaden ekosystem nie będzie działał dobrze, jeżeli klienci nie będą widzieli korzyści z korzystania z niego lub nie będą przekonani o jego wygodzie i bezpieczeństwie. Dlatego, dla skutecznej integracji otwartej bankowości potrzebna jest edukacja klientów.

A jakie jest ich nastawienie? Badania opinii pokazują, że są zainteresowani innowacjami, ale nie do końca rozumieją, jak działa nowy ekosystem i w związku z tym mają do niego ograniczone zaufanie. Zgodnie z wynikami zeszłorocznej ankiety Mastercard, 48% Polaków chciałoby używać aplikacji, która pozwala zarządzać kontami w różnych bankach, a 25% z takiej, która pozwala planować swoje wydatki na podstawie historii transakcji pochodzących z różnych źródeł. Ponadto 24% respondentów jest zainteresowanych korzystaniem z usług finansowych, które oferują daleko idącą personalizację, na podstawie danych z ich kont w różnych instytucjach.

Inne badania pokazują, że gotowość Polaków do udostępniania wrażliwych danych finansowych na swój temat jest ograniczona, szczególnie jeśli chodzi o mniejsze firmy finansowe, których nie znają. Poza tym Polacy nie do końca wiedzą, na czym polega bankowość otwarta, co dodatkowo zmniejsza ich poczucie bezpieczeństwa. W badaniu Mastercard tylko



23% z nich deklaruje, że dobrze rozumie, na czym polega ten ekosystem.

Tu pojawia się szansa dla banków, które od pokoleń są na szczycie listy instytucji budzących społeczne zaufanie, będące jednym z ich kluczowych zasobów. 65% respondentów w badaniu Mastercard odpowiada, że ich zaufanym źródłem informacji o zarządzaniu finansami są właśnie banki. Co więcej, zaufanie to jest jeszcze wyższe (71%) w najmłodszej grupie wiekowej (18–29 lat), która szczególnie chętnie korzysta z technologicznych nowinek.

Bezpieczeństwo na pierwszym miejscu

Aby budować zaufanie klientów do bankowości otwartej, a także zabezpieczać banki przed skutkami oszustw, potrzebne są nowe rozwiązania. W końcu otwarty obieg danych sprawia, że trudniej jest je chronić, a z zapytaniem o nie mogą zgłaszać się instytucje, z którymi partner bankowy wcześniej nie miał do czynienia.

W Mastercard chcemy pomagać w tworzeniu bezpiecznego środowiska dla bankowości otwartej, by stworzyć jak najlepsze warunki do rozwijania innowacyjnych rozwiązań oraz pomagać bankom i fintechom udostępniać te innowacje klientom. Dlatego właśnie stworzyliśmy wspomniany już pakiet usług Mastercard Open Banking Solutions. W jego skład wchodzi kilka rozwiązań, z których każde może wspierać bank w inny sposób:

Open Banking Connect – wspólne i wystandaryzowane API połączone z systemami otwartej bankowości instytucji finansowych, zapewniające dostawcom zewnętrznym skalowalność, elastyczność i szybkość

” Z analizy rozwiązań dostępnych już na świecie wynika, że najczęstsze sposoby wykorzystania otwartej bankowości przez tradycyjne banki to możliwość wykorzystania informacji dla optymalizacji procesów pożyczkowych, analityka pod kątem x-sellu i up-sellu produktów dla klientów (sprzedaż produktów komplementarnych i sprzedaż produktów posiadanych przez klienta w innej instytucji, na korzystniejszych warunkach), rozszerzona analityka pod kątem CRM i cyklu życia klienta.

wprowadzania nowych produktów na rynek.

Open Banking Protect – weryfikacja statusu rejestracji dostawcy zewnętrznego z Unii Europejskiej, połączona z monitorowaniem i generowaniem alertów w celu obniżenia ryzyka z tytułu odpowiedzialności i oszustw.

Open Banking Resolve – scentralizowana usługa do przetwarzania zapytań i rozstrzygania sporów, mająca zapewnić jasność, spójność i przejrzystość. Usługa wykorzystuje doświadczenie Mastercard w rozwiązywaniu krajowych i międzynarodowych reklamacji. W przypadku gdy strony nie mogą dojść do porozumienia między sobą, Mastercard oferuje niezależne wsparcie w zakresie arbitrażu.

Open Banking Consulting Services – profesjonalne doradztwo i praktyczne wsparcie pomagające instytucjom finansowym definiować i realizować ich strategię otwartej bankowości.

Podsumowując, ostatni rok pokazał, że otwarta bankowość przynosi bankom więcej szans niż ryzyk. To właśnie tradycyjni gracze mogą stać się głównymi wygranymi w efekcie zmian, jakie wprowadziła dyrektywa PSD2. Otwiera ona przed bankami możliwości oferowania nowych rodzajów usług i czerpania z nowych źródeł przychodów. Wreszcie jest dla nich szansą na cyfrową „ucieczkę do przodu”, a więc zwiększenie poziomu innowacyjności oferty, co pozwoli im skutecznie rywalizować z nowymi rodzajami konkurentów z sektora GAFA. Rozwój nowego ekosystemu wymaga jednak czasu, edukacji klientów, inwestycji w nowe rozwiązania i w bezpieczeństwo.

BANK w rzeczywistości PSD2



■ ARTUR SKALSKI

Senior Business
Solutions Manager
SAS Enterprise
Decisioning
& ModelOps

■ Obowiązująca w Polsce od września 2019 r. dyrektywa PSD2 jest kolejnym krokiem w kierunku ujednolicania rynku płatności w Unii Europejskiej. Ma na celu zwiększenie bezpieczeństwa w zakresie płatności elektronicznych, ale także wprowadza pojęcie otwartej bankowości, co oznacza możliwość świadczenia usług płatniczych przez certyfikowanych zewnętrznych dostawców. Mogą nimi być same banki lub inne instytucje płatnicze (potocznie zwane TPP – ang. *Third Party Providers*).

Patrząc na coraz bardziej złożony krajobraz różnorodnych usług finansowych i ich dostawców, możemy dostrzec trzy możliwe scenariusze odnalezienia się instytucji takiej, jak bank w rzeczywistości PSD2.

Scenariusz pierwszy

Tak naprawdę to właściwie poprzestanie na spełnieniu technicznych wymagań wynikających z przyjętej nowelizacją ustawy o usługach płatniczych dyrektywy PSD2, czyli udostępnienie certyfikowanym

podmiotom możliwości pobrania danych dotyczących rachunku klienta banku (oczywiście za jego zgodą) oraz wykonania w jego (klienta) imieniu operacji na rachunku prowadzonym przez bank. Oczywiście poza tymi dwoma aspektami jest jeszcze

szereg technicznych i proceduralnych wymogów, związanych chociażby z silnym uwierzytelnieniem, jakim musi sprostać bank jako podmiot odpowiedzialny za prowadzenie rachunku klienta i środki mu powierzone. Bardzo prawdopodobną konsekwencją pierwszego scenariusza jest utrata relacji z częścią z klientów banku na rzecz TPP.

TPP w imieniu i za zgodą klienta będzie przede wszystkim realizować dwie operacje: AIS (Account Information Service) oraz PIS (Payment Initiation Service). AIS pozwala na pozyskanie informacji o rachunkach klienta, natomiast PIS pozwala zlecić operację na rachunku w imieniu klienta banku. Bardzo łatwo zatem wyobrazić sobie sytuację, w której część klientów zacznie korzystać z aplikacji podmiotów trzecich (fintechów lub innych banków), zarządzając swoimi finansami. **Relacja banku z klientami budowana i utrzymywana za pośrednictwem własnych kanałów elektronicznych może zostać znacząco zredukowana, gdy konsumenci zaczną korzystać z rozwiązań podmiotu trzeciego.**

W konsekwencji można spodziewać się, że w dłuższej perspektywie przyczyni się to do utraty klientów lub też sprowadzi bank w relacji z klientem do poziomu podmiotu zapewniającego jedynie techniczną obsługę rachunku. Oznaczałoby to bardzo ograniczoną możliwość rozwoju klienta w zakresie portfolio produktów i podnoszenia jego wartości dla banku.

Aktywność na rynku usług finansowych firm Google czy Apple lub fintechów, jak Revolut, czyni wyżej opisane ryzyko jeszcze bardziej realnym. Revolut, startup założony w 2015 r., już w tej chwili, poza usługą wymiany walut,

oferuje założenie konta, ale przede wszystkim daje możliwość obsługi rachunków innych banków w swojej aplikacji mobilnej, aspirując do roli narzędzia pierwszego wyboru dla klientów tych banków w zakresie sprawnego zarządzania finansami.

Google w sierpniu br. ogłosił uruchomienie usług bankowych – możliwości otwarcia rachunku w ramach Google Pay, stąd już niedaleko do aplikacji pozwalającej na zarządzanie środkami na tym rachunku i dalej na podłączenie rachunków innych banków. Być może podobne ambicje będzie miał również Apple, który w tym samym miesiącu, we współpracy z Goldman Sachs, udostępnił swoim użytkownikom Apple Card.

” Relacja banku z klientami budowana i utrzymywana za pośrednictwem własnych kanałów elektronicznych może zostać znacząco zredukowana, gdy konsumenci zaczną korzystać z rozwiązań podmiotu trzeciego.

A zatem PSD2 poza bezpieczeństwem daje nieco więcej możliwości zarządzania finansami. Firmy spoza sektora bankowego zyskują szansę wejścia na rynek usług finansowych. Natomiast banki, poza obowiązkami regulacyjnymi, muszą stawić czoła dodatkowym wyzwaniom związanym z utrzymaniem klientów i zwiększeniem ich wartości.

Ważne jest monitorowanie zapytań pod kątem ich typu, celu i podmiotu, który je inicjuje w imieniu klienta. Zapytanie o saldo z aplikacji TPP integrującej finanse klienta to cenna informacja o samym kliencie oraz o możliwej zmianie preferencji co do sposobu zarządzania finansami.

Scenariusz drugi

Zakładając, że jako bank nie chcemy poprzestać wyłącznie na udostępnieniu danych o naszych klientach podmiotom trzecim, możemy albo bronić stanu posiadania, albo, co wydaje się być nieuniknione, aktywnie działać w środowisku PSD2 jako TPP.

Na czym miałyby polegać obrona stanu posiadania? Mówiąc najprościej, na monitorowaniu korzystania z dobrodziejstw PSD2 przez klientów własnych i odpowied-

” Ważne jest monitorowanie zapytań pod kątem ich typu, celu i podmiotu, który je inicjuje w imieniu klienta. Zapytanie o saldo z aplikacji TPP integrującej finanse klienta to cenna informacja o samym kliencie oraz o możliwej zmianie preferencji co do sposobu zarządzania finansami.

nim reagowaniu. Usługa AIS polegająca na udostępnieniu podmiotowi trzeciemu informacji dotyczących rachunku klienta banku – to usługa, dzięki której można również uzyskać dostęp do historii transakcji i wykorzystać ją w celu dokonania chociażby oceny zdolności kredytowej. Można zatem wyobrazić sobie scenariusz, w którym coraz więcej sklepów internetowych (a może i nie tylko internetowych) będzie chciało wdrażać usługi kredytowania zakupów w formie odroczonych płatności, a finalną decyzję dotyczącą uruchomienia takiej usługi oprzeć na analizie historii transakcji.

Jak może i powinien zareagować w takiej sytuacji bank? Po pierwsze – monitoring takich zdarzeń umożliwia identyfikację potrzeby kredytowej, na którą można reagować odpowiednią komunikacją. Oczywiście ważny jest czas reakcji i szybki kontakt z klientem. Systemy do zarządzania relacją z nim, wykorzystujące analizę strumieni zdarzeń, umożliwiają reagowanie na wydarzenia w czasie rzeczywistym i przygotowywanie spersonalizowanych ofert. Po drugie – jest to cenna informacja o zachowaniu klienta, o którą można wzbogacić mikrosegmentację klientów wykorzystywaną w kampaniach marketingowych.

Ważne jest monitorowanie zapytań pod kątem ich typu, celu i podmiotu, który je inicjuje w imieniu klienta. Zapytanie o saldo z aplikacji TPP integrującej finanse klienta to cenna informacja o nim samym oraz o możliwej zmianie preferencji co do sposobu zarządzania finansami. Należałoby dokonać oceny, na ile ta zmiana będzie trwała, albo czy będzie prowadzić do rezygnacji z korzystania

z kanałów własnych banku i finalnie utraty części wartościowej relacji z klientem. Warto również sprawdzić, ilu podobnych klientów jest w bazie i jaka jest szansa, że oni również zaczną korzystać z usług podmiotów trzecich i jaki finalnie może mieć to wpływ na ich lojalność oraz wartość dla banku. **Bank ma możliwość monetyzacji posiadanych zasobów: danych, infrastruktury i oprogramowania poprzez budowę i sprzedaż usług premium podmiotom trzecim.**

Wróćmy jeszcze do przykładu zapytania o historię transakcji w celu oceny zdolności kredytowej. Standard PolishAPI umożliwia realizację usług premium w ramach obsługi zapytań AIS. Oznacza to, że bank może nie tylko udostępnić dane, ale również oferować własne odpłatne usługi wobec TPP. W przypadku zapytania o historię w celu wydania decyzji kredytowej samo jej przetworzenie wymaga pewnej standaryzacji, agregacji i finalnie uruchomienia modelu analitycznego dostarczającego ocenę punktową ryzyka kredytowego.

Przykładowo sklepy występujące w roli TPP mogą nie dysponować narzędziami pozwalającymi na realizację tych operacji w czasie trwania sesji zakupowej. I tutaj pojawia się miejsce na usługę banku, który poza dostarczeniem historii rachunku może zaoferować również ocenę punktową ryzyka kredytowego, którą i tak wylicza na własne potrzeby z uwzględnieniem większej liczby danych niż historia transakcji na rachunku bankowym.

A zatem w scenariuszu drugim, który nazwaliśmy „obroną stanu posiadania”, bank może i powinien podejmować analizę kontaktów klientów z TPP i na jej podstawie realizować zadania mające na celu przeciwdziałanie utracie własnych relacji z klientem. Po drugie – ma możliwość monetyzacji posiadanych zasobów: danych, infrastruktury i oprogramowania poprzez budowę i sprzedaż usług premium podmiotom trzecim. **Kluczowe działania to analiza relacji klientów własnych z dostawcami zewnętrznymi, budowanie usług premium dla TPP w celu monetyzacji zasobów własnych oraz budowanie usług opartych na AIS i PIS dla swoich klientów we własnych kanałach elektronicznych.**

Scenariusz trzeci

Trzeci ze scenariuszy to wejście w rolę TPP wobec innych, konkurencyjnych banków. To plan najbardziej angażujący, wymagający inwestycji w środowisko API w celu realizacji usług AIS i PIS na rachunkach innych banków oraz rozwoju aplikacji w elektronicznych kanałach własnych. Daje on jednak możliwość umocnienia pozycji na rynku usług bankowych. Niektóre banki w Polsce decydują się już na ten model.

Własna aplikacja z możliwością integracji informacji o rachunkach z innych banków to na pewno sposób na utrzymanie relacji z klientem i szansa na rozwój. Oczywiście wydaje się, że sama informacja o saldzie oraz możliwość zlecania operacji na pozostałych rachunkach klienta w innych bankach to nieco za mało. Mile widziane byłyby usługi agregujące te informacje w postaci np. podsumowań wydatków w kategoriach (co już wiele banków proponuje w ramach aplikacji czy bankowości elektronicznych dla własnych rachunków, co również jest dostępne w aplikacji Revolut), pokazujące pewne trendy czy nawet podpowiadające działania odnośnie lepszego zarządzania finansami. Tego typu usługi wymagają oczywiście pewnych nakładów w zakresie przetwarzania danych z kont zewnętrznych, standaryzacji, połączenia z własnymi danymi, wspólnej kategoryzacji i analizy w celu dostarczenia atrakcyjnych dla klienta informacji.



Kluczowe działania to analiza relacji klientów własnych z dostawcami zewnętrznymi, budowanie usług premium dla TPP w celu monetyzacji zasobów własnych oraz budowanie usług opartych o AIS i PIS dla swoich klientów we własnych kanałach elektronicznych.

Integracja kont zewnętrznych klienta we własnych kanałach elektronicznych banku to również nowe źródło danych o nim, które za jego zgodą bank może wykorzystać do rekalkulacji oceny punktownej ryzyka kredytowego czy też pełniejszego zrozumienia zachowania klienta, w konsekwencji efektywniejszej personalizacji komunikacji marketingowej.

Mitygacja ryzyk i pełne wykorzystanie potencjału PSD2 z punktu widzenia relacji banku z klientami wydają się kluczowymi czynnikami wpływającymi na utrzymanie, a nawet rozwój pozycji rynkowej banku i budowanie przewagi konkurencyjnej. Kluczowe działania to analiza relacji klientów własnych z TPP, budowanie usług premium dla TPP w celu monetyzacji zasobów własnych oraz budowanie usług opartych na AIS i PIS dla swoich klientów we własnych kanałach elektronicznych.

Open banking a nadużycia

czyli jak bezpiecznie otwierać banki

Przepisy dyrektywy PSD2 weszły w życie we wrześniu ubiegłego roku i choć spodziewano się przełomu po jej wdrożeniu, ten jeszcze nie nastąpił. Wyobrażenia bankowych innowatorów dopiero nabiera śmiałości, a rynek z pewnością na bieżąco będzie weryfikował ich pomysły.



**AGNIESZKA
PIECHOCKA**
Customer Advisor
SAS Forensic
& Compliance Team



PSD2 to druga wersja dyrektywy o usługach płatniczych, na mocy której ustalono, że banki mają się otworzyć na podmioty trzecie. Nie wchodząc w szczegóły, wspomniane rozporządzenie nakazało, aby każdy dostawca rachunków płatniczych miał wystawiony interfejs dostępowy (w naszym kraju PolishAPI), który po spełnieniu określonych wymogów przez tzw. Third Party Providers (TPP) umożliwiałby wykonanie zasadniczo jednej z usług – tj. dostępu do informacji o rachunku (AIS) i/lub inicjacji płatności (PIS). Na tym właśnie bazuje pojęcie otwartej bankowości.

Nowe możliwości...

Część banków podeszła do unijnej dyrektywy PSD2 jak do kolejnego obowiązku legislacyjnego, który muszą spełnić. Jednak wraz z upływem czasu w obrębie tych instytucji powstaje coraz więcej wdrożeń opartych na otwartej bankowości. Pierwsze rozwiązanie, które zaproponowały banki, to dostęp do wielu rachunków bankowych za pośrednictwem jednej aplikacji (multibankowość). Konsekwencją dostępu do kont z innych banków na jednej platformie jest wykonywanie płatności z dowolnego banku czy scoring kredytowy oparty na danych automatycznie pobieranych ze

wszystkich rachunków udostępnionych przez klienta. Drugim rozwiązaniem dostępnym dzięki otwarciu się banków jest możliwość inicjowania płatności przez podmioty trzecie. Usługa ta ma w założeniu przyspieszyć wykonanie transakcji kupna (np. wysyłkę towaru przez sklep internetowy), daje bowiem gwarancję uzyskania zapłaty za towar lub usługi.

Nowe rozwiązania są szczególnie atrakcyjne dla osób posiadających konta w różnych instytucjach. Według raportu prnews.pl na koniec pierwszego kwartału 2020 r. Polacy

posiadali ok. 33,6 mln kont bankowych. Ponad połowa klientów (18 mln) aktywnie korzystała z bankowości internetowej, jednak zazwyczaj wszystko odbywało się w obrębie jednego banku. Drugi rachunek posiada wciąż niewielka część klientów (ok. 5%). Jednak ten odsetek będzie rósł wraz z nowymi możliwościami oferowanymi przez różne banki, które wykorzystując open banking, będą mogły zaproponować dostęp do innowacyjnych produktów i usług opartych na bazie najnowszych technologii, łatwiejsze zarządzanie finansami czy otrzymywanie ofert skrojonych na miarę potrzeb klienta.

...ale i nowe zagrożenia

Niestety, rewolucja jaka odbywa się obecnie w bankowości, otwiera nowe możliwości nie tylko dla użytkowników, ale również oszustów. **Otwarta bankowość wprowadziła zupełnie nowe zagrożenia, gdzie to właśnie klienci stają się bardziej podatni na atak cyberprzestępców.** Świadomość klientów dotycząca zagrożeń czyhających w internecie często jest niska, przez co stają się łatwym celem dla grup przestępczych, które pragną uzyskać dostęp do poufnych danych oraz potwierdzenia nieuprawnionych transakcji.

Wyzwaniem staje się więc maksymalne utrudnienie przestępcom dostępu do danych użytkownika w procesie przeprowadzania transakcji. Jednym ze środków wprowadzonych przez dyrektywę PSD2 w celu zwiększenia bezpieczeństwa płatności internetowych jest silne uwierzytelnianie klienta (ang. *strong customer authentication* – SCA). Przepisy te wymagają weryfikacji tożsamości kupującego przed umożliwieniem dokonania zakupu online.



”

Poprzez wykorzystanie biometrii, analizy behawioralnej czy zbierania danych o urządzeniu (ang. *device fingerprint*), na podstawie wcześniejszych zachowań klientów w konkretnych sytuacjach możliwe jest wykrycie odchyłeń od wzorca, będących podstawą do głębszej analizy.

Podmiot autoryzujący transakcję online musi potwierdzić tożsamość klienta, wykorzystując co najmniej dwa z następujących sposobów:

- coś, co użytkownik posiada (np. telefon lub tablet),
- coś, czym użytkownik jest (np. rozpoznawanie twarzy lub odcisk palca),
- coś, co użytkownik wie (np. PIN lub hasło).

Przy bardziej skomplikowanym procesie uwierzytelnienia banki stają przed wyzwaniem optymalizacji z perspektywy doświadczeń klienta, tak by móc zachować balans między bezpieczeństwem transakcji a zadowoleniem konsumenta, który daną transakcję chce wykonać. Zagadnienie to otwiera nowe możliwości dla firm z sektora fintech. **Poprzez wykorzystanie biometrii, analizy behawioralnej czy zbierania danych o urządzeniu (ang. *device fingerprint*), na podstawie wcześniejszych zachowań klientów w konkretnych sytuacjach możliwe jest wykrycie odchyłeń od wzorca, będących podstawą do głębszej analizy.** Zbierane w ten sposób dane przyczyniają się do usprawniania systemów antyfraudowych – scoring poszczególnych transakcji staje się bardziej trafny, co w konsekwencji przekłada się na zmniejszenie ilości udanych oszustw bankowych.

Najważniejsze jest bezpieczeństwo

Odchodząc od perspektywy pojedynczego klienta, spójrzmy na open banking ze strony banków. Potencjalna współpraca z podmiotami trzecimi (TPP) niesie za sobą wiele korzyści. Świeże spojrzenie na wewnętrzne procesy banku pod kątem ich usprawnienia, efektywne wykorzystywanie danych o klientach, np. w zakresie oceny ryzyka czy zwinne podejście we wdrażaniu nowych rozwiązań – to tylko niektóre z nich. Jednak nie brakuje również zagrożeń. Musimy pamiętać, że za dane osobowe klientów i ich środki zgromadzone na kontach bankowych w dalszym ciągu odpowiadają prowadzące je instytucje. Dlatego ważne jest, aby banki mogły szybko weryfikować polecenia inicjacji płatności i informacji o rachunku otrzymywane w ramach infrastruktury otwartej bankowości od dostawców zewnętrznych (TPP).

Na rynku europejskim z miesiąca na miesiąc pojawia się coraz więcej nowych podmiotów wykorzystujących możliwości otwartej bankowości. I choć ten trend nie jest jeszcze widoczny w Polsce, z pewnością w najbliższych miesiącach pojawią się nowe podmioty, z którymi instytucje zarządzające kontem nie miały wcześniej do czynienia. Każde dodatkowe ogniwo podczas przeprowadzania transakcji zwiększa jej ryzyko. **W miarę poszerzania się grona dostawców zewnętrznych rośnie zagrożenie wycieku/przywłaszczenia danych przez jeden z podmiotów i wykorzystania ich np. przy wyludzeniach kredytowych.** Innym czarnym scenariuszem jest bezpośrednie zagrożenie utraty środków po zleceniu płatności przez TPP. Podmioty trzecie są bardziej narażone na zostanie ofiarą

RYS. 1. Wzrost bezpieczeństwa dzięki otwartej bankowości



RYS. 2. Zagrożenia otwartej bankowości



cyberprzestępstwa, a w skrajnych przypadkach, gdy certyfikowanych TPP będzie już bardzo dużo – przestępcy z pewnością będą próbować podszywać się pod legalne TPP lub zakładać nowe, od początku w celu wyludzenia pieniędzy.

Właśnie w takich sytuacjach niezbędna jest dodatkowa weryfikacja. Potrzebne są niezawodne systemy, które dzięki wykorzystaniu zaawansowanej analityki w czasie rzeczywistym są w stanie wykrywać wczesne sygnały ostrzegawcze, wskazujących anomalie i potencjalne oszustwo.

Dostawcy usług płatniczych szukają optymalnej równowagi między redukcją fałszywych alarmów, które mogą powodować niepotrzebne

utrudnienia dla klientów, a brakiem wykrycia przestępstwa, co może prowadzić do strat finansowych. Zgodnie z ustawą PSD2 obniżona została kwota, którą może być obciążony klient w przypadku kwestionowanej transakcji – odpowiedzialność zostaje zatem przerzucona w większym stopniu na pośredników w płatnościach. W przypadku transakcji bez SCA odpowiedzialność za nieautoryzowaną transakcję ponosi w całości dostawca usług płatniczych.

Zaawansowane metody analityczne

Aby dostosować się do nowych realiów, warto skorzystać z rozwiązań opartych na zaawansowanych metodach analitycznych. Skuteczna platforma

do przeciwdziałania oszustwom w erze otwartej bankowości powinna składać się z następujących komponentów:

Centrum decyzyjne. Jeden centralny ośrodek decyzyjny, który łącząc dane z różnych źródeł zapewnia ujednolicony obraz konta/podmiotu podczas całej transakcji.

Analiza zdarzeń niepieniężnych.

Zachowanie w trakcie sesji może wiele powiedzieć o użytkowniku. Większość użytkowników online/mobilnych ma regularne wzorce interakcji ze sprzedawcami i portalami finansowymi. Korzystają z podobnych wzorców nawigacji i niewielkiej liczby urzędzeń. Odejście od przyzwyczajenia może sygnalizować nieuprawniony dostęp. Silny system autoryzacji może wychwytywać wzorce zachowań użytkowników z wielu źródeł i oceniać je za każdym razem, gdy transakcja płatnicza jest wykonywana.

Analiza hybrydowa. Łącząc wiele metod analitycznych, można dokładniej rozróżniać legalnych użytkowników od oszustów. Wykrywanie anomalii i analizy predykcyjne pomogą odkryć nowe formy ryzyka poprzez zbadanie tego, co dzieje się teraz. Sieci powiązań mogą wskazać na znowę lub rozbieżności, które stanowią potencjalne sygnały ostrzegawcze, a nawet przestępczość zorganizowaną. Wykorzystanie reguł eksperckich pozwala – na podstawie doświadczeń pracowników banku – na lepsze typowanie podejrzanych podmiotów.

Uczenie maszynowe. W przeciwieństwie do systemów opartych tylko na regułach, które oszuści mogą łatwo prze-testować i obejść, uczenie maszynowe dostosowuje się do zmieniających się zachowań w populacji poprzez

RYS. 3. Platforma do przeciwdziałania nadużyciom



zautomatyzowane budowanie modeli. Z każdą iteracją algorytmy stają się inteligentniejsze i zapewniają dokładniejsze wyniki. Łatwo jest dostrzec wartość uczenia maszynowego, aby nadążyć za pojawiającym się ryzykiem związanym z nowymi podmiotami, które mogą inicjować płatności.

Integracja danych niestandardowych.

Istnieje niezliczona liczba różnych sposobów przekształcania, wzbogacania, sprawdzania i przechowywania danych zebranych podczas transakcji – które są dostępne w wielu formatach, gdyż pochodzą z różnych źródeł. Otwarta bankowość pozwala na wzbogacenie ich m.in. o dane biometryczne, behawioralne czy pochodzące z wykorzystywanych urzędzeń.

Zarządzanie alertami. System powinien inteligentnie ustalać priorytety alertów do segregacji, dochodzenia i usunięcia. Analitycy śledczy muszą szybko dostrzec potencjalne obszary zagrożenia i na nich skupić się w pierwszej kolejności.

Zintegrowane zarządzanie przypadkami. Wspólny system zarządzania

sprawami ułatwi współpracę i udostępnianie danych, a także kompleksowe śledzenie i audytowanie spraw. Odpowiednia platforma wspomaga pracowników, automatyzując procesy, które tradycyjnie były wykonywane ręcznie i nadając priorytet sprawom o największej wartości. Dzięki temu analitycy spędzają mniej czasu na przetwarzaniu danych, a więcej na badaniu i podejmowaniu działań w przypadku znaczących alertów.

Otwarta bankowość bez wątpienia niesie za sobą nowe rozwiązania i pomysły, które na naszych oczach będą zmieniać rynek finansów. Trzeba jednak mieć na uwadze, że klienci nie będą skłonni z nich korzystać, dopóki nie upewnią się, że są to rozwiązania bezpieczne i nie stanowią ryzyka dla ich finansów. Dostawcy usług płatniczych powinni inwestować w walkę z nadużyciami, by skutecznie chronić się zarówno od strat finansowych jak i reputacyjnych. Raz utracone zaufanie klientów bardzo trudno jest odbudować, a jak mówi stare polskie przysłowie, szczególnie aktualne w dzisiejszych czasach – lepiej zapobiegać, niż leczyć.

Open banking

CZYLI DWIE I PÓŁ USŁUGI + API

Jak trafnie i krótko scharakteryzować drugą dyrektywę w sprawie usług płatniczych (PSD2)?¹ Wielu pewnie by powiedziało, że głównie rewolucjonizuje ona europejski sektor płatniczy, zwłaszcza poprzez otwarcie na tak czy inaczej rozumiany fintech. Pierwsze niemal trzy lata od rozpoczęcia stosowania PSD2² skłaniają jednak do refleksji, że dyrektywa ta stanowi bardziej wstęp, preludium do dalszego rozwoju koncepcji otwartej bankowości (open banking), lub szerzej – jak zwykło się to ostatnio określać – otwartych finansów (open finance).



■ DR WOJCIECH IWAŃSKI

Senior counsel, adwokat

Z kancelarią SK&S współpracuje od 2006 r. Specjalizuje się w regulacji usług finansowych, przede wszystkim bankowych i płatniczych. Zajmuje się zagadnieniami dotyczącymi podejmowania i prowadzenia działalności przez polskie i zagraniczne podmioty w sektorze usług bankowych, płatniczych oraz maklerskich. Reprezentuje klientów w postępowaniach przed KNF, w tym w związku z nabywaniem polskich podmiotów regulowanych. Uczestniczył w wielu projektach outsourcingu regulowanego oraz wdrażania nowych technologii w bankowości i usługach płatniczych, w tym korzystania z cloud computingu, innowacyjnych płatności oraz wirtualnych walut. Laureat konkursu „Rising Star” (2015). W 2020 r. wyróżniony w prestiżowym rankingu Chambers & Partners – w kategoriach FinTech Legal oraz Banking & Finance.



■ MATEUSZ BLOCHER

Senior associate

Z kancelarią SK&S związany od 2009 r. Specjalizuje się w prawie bankowym publicznym i prywatnym, ze szczególnym uwzględnieniem problematyki usług płatniczych i AML. Zajmuje się doradztwem dla banków i innych instytucji sektora finansowego w zakresie regulacyjnym oraz transakcyjnym. Prowadził wiele procesów wdrożeniowych, w tym z zakresu PSD2, PAD oraz AMLD IV. Jest autorem ogólnopolskich publikacji naukowych dotyczących zmian regulacyjnych w bankowości.

PSD2 i potrzeba otwarcia bankowości

Od chwili wejścia w życie pierwszej dyrektywy w sprawie usług płatniczych (PSD1), co w większości państw członkowskich miało miejsce ponad dekadę temu³, rynek usług płatniczych, w tym paleta dostępnych na nim usług i produktów, przeszedł niewyobrażalną zmianę. Dynamiczny rozwój sektora, gdzie pierwsze skrzypce zagrały rozwój e-commerce, wzrost liczby płatności elektronicznych (w tym mobilnych), szerokie ubankowanie społeczeństwa oraz pojawienie się nowych, niebankowych uczestników rynku, stanowiły naturalne tło dla przyjęcia PSD2. Do najważniejszych zmian wprowadzonych nową dyrektywą należy „otwarcie” bankowości na nowe usługi płatnicze i na niebankowych ich dostawców.

- ¹ Dyrektywa 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego.
- ² Zgodnie z art. 115 ust. 2 PSD2, dyrektywa ta powinna być stosowana przez państwa członkowskie od 13 stycznia 2018 r.
- ³ PSD1 weszła w życie 25 grudnia 2007 r., z terminem implementacji do 1 listopada 2009 r. Polska implementacja była tradycyjnie opóźniona, w tym przypadku o niemal dwa lata.

Jak to otwarcie zostało zrealizowane? Głównie polegało na określeniu ram regulacyjnych dla dwóch nowych – w ujęciu prawnym, bo z perspektywy rynku w różnych formach były znane już wcześniej – usług płatniczych, tj. usługi dostępu do informacji o rachunku (AIS; Account Information Service) oraz usługi inicjowania transakcji płatniczej (PIS; Payment Initiation Service). W pewnym skrócie, usługa AIS pozwala zapewnić użytkownikowi usług płatniczych przez jednego dostawcę dostępu do informacji o rachunku lub rachunkach płatniczych tego użytkownika prowadzonych przez innego dostawcę usług płatniczych. Usługa PIS umożliwia z kolei inicjowanie zlecenia płatniczego przez dostawcę świadczącego tę usługę z rachunku płatniczego prowadzonego dla użytkownika przez innego dostawcę. Trzecią, choć nie do końca usługą, tym bardziej nie do końca usługą płatniczą i w dodatku nie do końca uregulowaną przez PSD2, ale za to na pewno nową dla większości uczestników rynku, jest tzw. funkcjonalność CoF (*confirmation of funds*; niekiedy określana jako CAF – *confirmation on the availability of funds*). Funkcjonalność ta pozwala na potwierdzanie przez dostawcę prowadzącego rachunek płatniczy dostępności salda na tym rachunku i przekazywania tej informacji do innego dostawcy wydającego instrumenty płatnicze oparte na karcie (CBPII).

Nieco z przymrużeniem oka można więc powiedzieć, że PSD2 to w praktyce dwie i pół nowej usługi. Te dwie i pół nowej usługi miało na celu otwarcie ugruntowanego środowiska dotychczasowych dostawców usług płatniczych na nowych dostawców. Ci nowi dostawcy uzyskali normatywne



” Boisko do gry w otwartą bankowość wygląda może nie jak krajobraz po bitwie, ale na pewno jak miejsce niejednej potyczki. Bramki są nieco poprzestawiane, lakier już nie taki błyszczący, linie trochę krzywe, a sponsor stadionu nieoczywisty.

gwarancje swobodnego świadczenia przez nich nowych usług. Ich trzon stanowi dostęp do rachunków płatniczych prowadzonych przez innych dostawców – w szczególności banki. Wypada jednak pamiętać, że PSD2 to nie tylko stworzenie ram prawnych dla otwartej bankowości. To także szereg innych zmian w dotychczasowych zasadach świadczenia usług płatniczych, w tym w zakresie odpowiedzialności za nieautoryzowane transakcje płatnicze, rozpatrywania reklamacji czy środków bezpieczeństwa.

Nowe role: ASPSP i TPP

W efekcie zmian wprowadzonych przez PSD2 dotychczasowy podział na bankowych i niebankowych dostawców usług płatniczych stracił nieco na znaczeniu. Choć rozróżnienie to w dalszym ciągu jest doniosłe (z mocy



Ostatnie dwa lata na polskim rynku płatniczym pokazały, że pomimo początkowego oporu ze strony niektórych banków wobec jakiegokolwiek otwarcia bankowości, dostawcy bankowi co do zasady stali się głęboko zainteresowani możliwością świadczenia nowych usług (AIS, PIS). Z tego jednak względu, że były to usługi całkowicie nowe w świetle litery prawa, konieczne było przeprowadzenie stosunkowo długotrwałych procesów licencyjnych przed Komisją Nadzoru Finansowego, związanych ze zmianą ich statutów. Wielu bankom udało się jednak z sukcesem zakończyć takie

postępowania (wśród nich znalazły się m.in. Alior Bank, mBank, Nest Bank, PKO BP i Santander Bank Polska). Na rynku pojawili się jednocześnie licencjonowani niebankowi dostawcy, którzy uprawnieni są do świadczenia usług AIS lub PIS (wśród nich m.in. Banqware, Blue Media, eCard, Kontomatik, Krajowy Integrator Płatności, mElements, Paymento Financial, PayPro, PayU, Profekasa, Ramp Link).

Mamy już zatem graczy. A jak wygląda boisko do otwartej bankowości?

Open banking, czyli jak pogodzić (rozbieżne) interesy

Boisko do gry w otwartą bankowość wygląda może nie jak krajobraz po bitwie, ale na pewno jak miejsce niejednej potyczki. Bramki są nieco poprzestawiane, lakier już nie taki błyszczący, linie trochę krzywe, a sponsor stadionu nieoczywisty. Dlaczego tak jest?

To wynik kilkuletnich dyskusji na szczepku europejskim odnośnie kształtu otwartej bankowości. A może

prawa podmiot będący bankiem może bowiem świadczyć pewne usługi, które nie są dostępne niebankowym dostawcom), to jego praktyczne zastosowanie gubi się nieco w realiach otwartej bankowości. Zasadnicza oś podziału to obecnie rozróżnienie na tych dostawców, którzy w danym układzie prowadzą rachunek płatniczy (ASPSP; Account Servicing Payment Service Provider) oraz na tych, którzy – w konkretnym przypadku – takiego rachunku nie prowadzą i z tego tytułu można określić ich jako dostawców trzecich (TPP; Third Party Provider).

Żonglując nieco tymi skrótowcami, można postawić pytanie, czy ASPSP może być jednocześnie TPP, a TPP jednocześnie ASPSP oraz czy są takie ASPSP, które nie są TPP i czy są takie TPP, które nie są ASPSP? Odpowiadając krótko – tak. Dostawcy usług płatniczych – oczywiście w zależności od tego, na świadczenie jakich usług posiadają zezwolenie – mogą występować w różnych rolach filmu pt. „otwarta bankowość”. Wszystko związane jest z konkretną interakcją, jaka zachodzi między dostawcami.

Niektórzy dostawcy (np. banki) z reguły występująć będą w roli ASPSP – to oni prowadzą bowiem rachunek płatniczy, do którego dostęp chce uzyskać dostawca trzeci (TPP). Tacy ASPSP sami mogą być jednak zainteresowani świadczeniem usług opartych na dostępie do rachunków płatniczych prowadzonych przez innych ASPSP. W takim przypadku, mogą oni jednocześnie występować w roli TPP. Są jednak i tacy ASPSP, którzy nie będą świadczyć usług jako TPP. Choć jest to nietypowe dla polskiego rynku usług płatniczych, możliwe są również przypadki, gdy podmiot z reguły działający w roli TPP (najczęściej dostawca niebankowy), będzie jednocześnie ASPSP. Chodzi tu przykładowo o instytucje płatnicze, które świadczą usługi AIS lub PIS i korzystają z dostępu do rachunków prowadzonych przez ASPSP, ale jednocześnie same prowadzą rachunki płatnicze dla swoich klientów i z tego tytułu występują w roli ASPSP. Nie można więc stawiać znaku równości między ASPSP i bankiem, tak samo jak nie można stawiać znaku równości między TPP i dostawcą niebankowym.

nawet nie tyle odnośnie jej kształtu, co raczej odnośnie praktycznych aspektów świadczenia nowych usług przez dostawców w roli TPP. W skrócie chodzi o API (*application programming interface*). Po przyjęciu PSD2 nie od razu było bowiem wiadomo, na jakiej zasadzie dostawcy trzeci mają uzyskiwać dostęp do rachunków płatniczych prowadzonych przez ASPSP w celu świadczenia nowych usług (AIS, PIS). Sama dyrektywa tego obszaru nie reguluje i pozostawia miejsce dla dookreślenia mechanizmów dostępu do rachunków rozporządzeniu delegowanemu 2018/389 (RTS). Obecny kształt RTS-ów to efekt kilku szkiców na przemian opracowanych przez Europejski Urząd Nadzoru Bankowego (EUNB; European Banking Authority) oraz Komisję Europejską. Wzajemna korespondencja pomiędzy nimi wyraźnie pokazuje, że jedną z głównych osi sporu (lub mówiąc łagodniej – braku porozumienia) była mechanika dostępu do rachunków płatniczych.

Punktem wyjścia do dyskusji było utrzymanie dotychczasowej (sprzed PSD2) praktyki rynkowej, która w znacznej mierze opierała się na nierejestrowanym dostępie TPP do rachunku płatniczego w celu pozyskania danych o nim na podstawie danych dostępowych klienta i dzięki metodzie screen scrapingu. Taka formuła dostępu zakładała, że TPP uzyskuje dostęp do rachunku tak jakby był użytkownikiem. Utrzymanie dotychczasowych metod dostępu miało zapewnić w ocenie wielu uczestników rynku płynne przejście ze środowiska nieregulowanego do środowiska poddanego ograniczeniom PSD2, bez jednoczesnego zachwiania istniejących modeli biznesowych.

EUNB odrzucił jednak ten wariant. Jeden z pierwszych projektów RTS-ów⁴, który został opracowany przez EUNB, zakładał, że komunikacja na linii TPP–ASPSP ma odbywać się za pośrednictwem przeznaczonych do tego interfejsów. Alternatywnie mógł być to zmodyfikowany interfejs dostępu bezpośredniego (z którego użytkownicy usług płatniczych korzystają na co dzień) lub interfejs dedykowany – potocznie określany jako API. ASPSP mieli być jednocześnie zobligowani do przygotowania planów awaryjnych, które zapewnią TPP możliwość ciągłego świadczenia usług opartych na dostępie do rachunku w przypadku, gdyby API było niedostępne z powodu nieplanowanych przerw lub awarii systemowych.

” Praktyką niedozwoloną jest natomiast uzyskiwanie przez TPP dostępu do rachunków płatniczych prowadzonych przez ASPSP za pomocą metod innych niż API, zmodyfikowany interfejs dostępowy lub udostępniony przez ASPSP mechanizm fallback (na wypadek niedostępności API).

Tak skonstruowane założenia mechaniki dostępu do rachunków prowadzonych przez ASPSP spotkały się z krytyką Komisji Europejskiej. W piśmie z 24 maja 2017 r., zarzuciła ona EUNB, że ówczesny projekt RTS-ów nie pozwalał na właściwe zabezpieczenie interesów biznesowych TPP przed nieprzewidywanymi problemami z funkcjonowaniem API. Taki sytuację, przy jednoczesnym braku wystąpienia problemów z interfejsami dostępu bezpośredniego klientów ASPSP, mogłyby prowadzić do dyskryminacji TPP i stopniowego zniechęcania klientów do korzystania z ich usług. Środkiem zaradczym, którego zażądała KE, było przygotowanie przez ASPSP środków dostępu awaryjnego opartych na interfejsach udostępnionych klientom do bezpośredniego użytku (*user-facing interface* albo *customer interface*). Było to tzw. opcja *fall-back* (*fallback option*).

4 EBA/RTS/2017/02 z 23.02.2017 r.



Podejście zaprezentowane przez Komisję Europejską spotkało się z kolei z krytyką EUNB. W opinii z 29 czerwca 2017 r. urząd zaszygnował, że o ile zgadza się z potrzebą wprowadzenia mechanizmów antydyskryminacyjnych w stosunku do TPP, o tyle obowiązek ustanowienia przez ASPSP opcji fallback wydaje się nie być dobrym ku temu instrumentem i wykracza poza mandat do wydania rozporządzenia delegowanego zgodnie z PSD2. EUNB podkreślił, że wprowadzenie wymogów w zakresie opcji fallback będzie pociągało za sobą szereg negatywnych konsekwencji, w tym dodatkowe koszty po stronie ASPSP, fragmentaryzację rynku oraz ryzyko braku zgodności z normami bezpieczeństwa wyznaczonymi przez PSD2.

Ostatecznie wypracowano rozwiązanie kompromisowe. ASPSP mogą obecnie wybrać, czy wystawią dla potrzeb TPP dedykowany interfejs dostępowy (API), czy też odpowiednio zmodyfikują istniejący interfejs wykorzystywany przez klientów do bezpośredniego dostępu do rachunku.

Gdy jednak zdecydują się wystawić API, opracowane przez nich plany awaryjne powinny uwzględniać mechanizm fallback, który pozwoli TPP na ciągłe świadczenie usług w przypadku niedostępności lub awarii API. Pod warunkiem spełnienia określonych kryteriów, w szczególności wykazania, że API jest należycie zaprojektowane i zabezpieczone, ASPSP mogą uzyskać zwolnienie spod obowiązku ustanowienia mechanizmów fallback. A contrario, praktyką niedozwoloną jest natomiast uzyskiwanie przez TPP dostępu do rachunków płatniczych prowadzonych przez ASPSP za pomocą metod innych niż API, zmodyfikowany interfejs dostępowy lub udostępniony przez ASPSP mechanizm fallback (na wypadek niedostępności API).

Znaczenie standardów rynkowych dla rozwoju open bankingu

Choć pożądana metoda dostępu do rachunków przez TPP została ostatecznie przesądzona w ramach RTS-ów, to szczegółowe wymaga-

nia co do kształtu API nie zostały formalnie uregulowane. W tym zakresie kluczową rolę odegrały inicjatywy rynkowe, których celem było wypracowanie jednolitych, dobrych standardów API.

Dla polskiego rynku kluczowe znaczenie ma standard wypracowany pod auspicjami Związku Banków Polskich – PolishAPI. Podstawowym jego celem jest zdefiniowanie modelowego interfejsu dostępowego służącego do świadczenia usług otwartej bankowości, w tym określenie szczegółowych zasad komunikacji na linii ASPSP–TPP.

W wypracowaniu standardu PolishAPI brały udział nie tylko banki, ale także wiele uczestników niebankowych. Taki tryb projektowania miał zapewnić odpowiednie wyważenie standardu i pogodzenie ze sobą potrzeb wszystkich uczestników sektora płatniczego. Co istotne, w celu zabezpieczenia interesów TPP, prace nad standardem zostały „zabezpieczone” pewnymi mechanizmami regulacyjnymi. Pod kątem zgodności

z prawem standard PolishAPI był poddawany ocenie Narodowego Banku Polskiego. Przyjęcie pierwszej jego wersji było poprzedzone szerokimi i stosunkowo długimi konsultacjami publicznymi. Projekt ma charakter żywy – cały czas trwają prace nad kolejnymi wersjami standardu, uwzględniające pojawiające się nowe interpretacje przepisów, wytyczne interpretacyjne prawnej grupy roboczej ZBP ds. PSD2⁵ oraz potrzeby rynku. W literaturze europejskiej model współpracy pomiędzy Związkiem Banków Polskich i uczestnikami rynku oceniany jest pozytywnie jako sposób redukcji globalnych kosztów związanych z implementacją PSD2⁶.

Choć standardy rynkowe w obszarze otwartej bankowości nie mają żadnej wiążącej mocy, a zgodność ze standardami nie oznacza jeszcze sama przez się zgodności z prawem, to w praktyce odgrywają one kluczową rolę dla ukształtowania zasad świadczenia nowych usług. W Polsce zdecydowana większość banków podjęła decyzję o oparciu swoich specjalnych interfejsów dostępowych właśnie na standardzie PolishAPI. Ujednolicony standard oraz modelowy wniosek o zwolnienie spod opcji fallback, który również został wypracowany w ramach Związku Banków Polskich, niewątpliwie usprawnił toczące się przed Komisją Nadzoru Finansowego postępowania związane z uzyskaniem przez ASPSP

zwolnień spod obowiązku ustanawiania mechanizmów awaryjnych (fallback).

PSD2 open API – co dalej?

Wdrożenie API przez ASPSP było nie lada wyzwaniem regulacyjnym. Prawdłowo skonstruowany interfejs dostępowy musi bowiem spełniać szereg wymogów przewidzianych w PSD2, RTS-ach oraz wytycznych EBA. Punktem kulminacyjnym dla procesów wdrożeniowych były przeprowadzane przez zewnętrznych doradców – najczęściej prawnych i technologicznych – audyty zgodności API z ramami regulacyjnymi. Pokazały one, że znaczna część dostawców prowadzących rachunki dołożyła starań, aby odpowiednio przygotowywać swoje interfejsy. Wiele obszarów budziło jednak wątpliwości – tak w zakresie praktycznych aspektów wdrożenia – jak i pod kątem niejasnych ram prawnych. Do tej pory może na przykład zastanawiać, na jakiej podstawie EUNB oczekuje

” Zrealizowane przez ASPSP wdrożenia tych standardów prędzej czy później również będą musiały być poddane okresowym sprawdzeniom. W jakim zakresie i na jakich warunkach? Tego nie da się z góry przesądzić.

udostępnienia przez ASPSP dla dostawców usług PIS funkcjonalności CoF (w środowisku problem potocznie określany jest jako „CoF w PIS-ie”; powoływane przez EUNB podstawy prawne należałoby raczej uznać za niewystarczające).

Nie powinno jednak budzić wątpliwości, że faktyczny wymiar świadczenia usług w ramach otwartej bankowości będzie podlegał naturalnym zmianom. Lustrzanym odbiciem tych zmian są i będą modyfikacje standardów rynkowych. Zrealizowane przez ASPSP wdrożenia tych standardów prędzej czy później również będą musiały być poddane okresowym sprawdzeniom. W jakim zakresie i na jakich warunkach? Tego nie da się z góry przesądzić. Być może jest to kolejne pole dla modelowej współpracy sektora z Urzędem Komisji Nadzoru Finansowego.

5 Aktualna wersja wytycznych zawarta została w piśmie ZBP z 1 października 2019 r.

6 Zob. np. O. Borgogno, G. Colangelo, Data, Innovation and Competition in Finance: The Case of the Access to Account Rule, EU Law Working Papers No. 35, Stanford-Vienna Transatlantic Technology Law Forum (2018).

