

Beyond AI: W stronę Agentic Banking



Technologie, regulacje i architektura płatności
kształtujące nową erę autonomicznych finansów.

Spis treści

Od autorów	3
Executive Summary	4
Jak badaliśmy rynek – źródła, metoda i ograniczenia analizy	5
Czym jest Agentic Banking i na jakim etapie jest rynek	7
Granice prawne i regulacyjne	14
Technologia i koszty – co napędza, a co blokuje wdrożenia	22
Nowe protokoły płatnicze – jak Visa, Mastercard i Stripe budują infrastrukturę dla agentów	26
Nowe zagrożenia – jak przestępcy wykorzystują AI przeciwko bankom	33
Najlepsze przykłady z rynku	36
Plan działania – co wdrożyć teraz, a co może poczekać	39
Konkluzja	41

Od autorów

Raport „Beyond AI: W stronę Agentic Banking” porządkuje wiedzę o najszybszych transformacjach finansowego sektora.

Stworzyliśmy praktyczny przewodnik łączący **trzy kluczowe perspektywy**:



Regulacyjna perspektywa określa dopuszczalne działania.



Technologiczna perspektywa wskazuje dostępne możliwości.



Biznesowa perspektywa ocenia rynkową opłacalność.

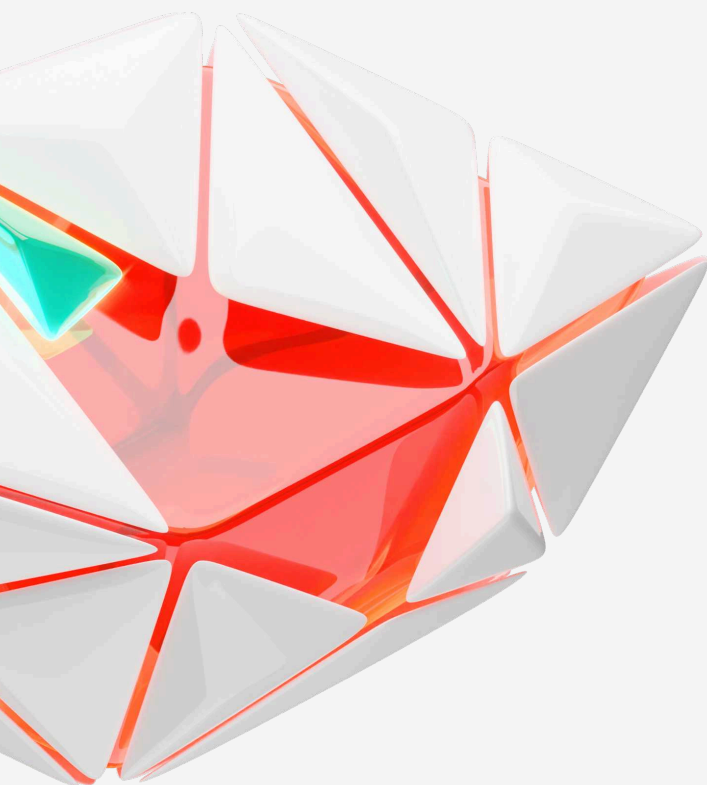
Staramy się przy tym zachować krytyczną postawę i kwestionujemy powszechny, a miejscami ślepy entuzjazm dotyczący sztucznej inteligencji. Właśnie dlatego postanowiliśmy opisać wyłącznie działające rozwiązania – takie, które zachowują ścisłą zgodność z europejskim prawem i przynoszą mierzalne korzyści.

Mamy nadzieję, że tak zarysowana perspektywa okaże się pomocna dla decydentów w bankach, firmach technologicznych i instytucjach finansowych – a przede wszystkim ułatwi im odpowiedzialne wdrażanie systemów Agentic Banking przy pełnym zachowaniu kontroli nad ryzykiem i danymi, bez uszczerbku na zaufaniu klientów



Michał Grela

Head of Growth



Executive Summary

Rok 2026 nie przyniesie w pełni autonomicznych rozwiązań z zakresu Agent Banking. Zamiast tego będziemy świadkami rozwoju inteligentnych systemów, które potrafią zrozumieć cel, a następnie samodzielnie zaplanować i wykonać potrzebne działania. Wszystko to będzie się jednak odbywać w zdefiniowanych przez legislatorów granicach - systemy te zawsze będą działać wyłącznie na podstawie zgód klienta, przestrzegając przy tym procedur bankowych. Dane EBA i Bank of England, a także ustalenia FCA potwierdzają szerokie wdrażanie AI w europejskich bankach, przy jednoczesnym minimalnym stopniu faktycznej autonomii. Obecnie tylko 2% zastosowań sztucznej inteligencji w sektorze finansowym ma charakter w pełni samodzielny. W praktyce niemal każde działanie AI w bankowości odbywa się dziś pod kontrolą człowieka.

Równolegle Visa i Mastercard w oparciu o tokenizację oraz weryfikację tożsamości agentów tworzą

bezpieczną infrastrukturę pozwalającą na delegowanie uprawnień. Kluczowe są tu jasno określone limity i bieżąca kontrola każdej transakcji.

Należy podkreślić, że Agent Banking wykracza w tej chwili daleko poza funkcje zaawansowanych chatbotów. Agenci AI nie tylko odpowiadają na pytania, ale w coraz większym zakresie potrafią samodzielnie planować i koordynować złożone procesy finansowe – choć zawsze w ramach zdefiniowanych uprawnień i pod nadzorem człowieka. Ze względu na tak dużą decyzyjność, sama „sprawność” technologii nie wystarczy, aby przekonać klientów do powierzenia systemom swoich pieniędzy. Przewagę na rynku zbudują więc te banki, które oprócz wdrożenia innowacji zagwarantują pełną kontrolę i bezpieczeństwo - dopracowując system zgód klienta, zapewniając transparentność działania algorytmów oraz rygorystyczną kontrolę ryzyka.

92%

Banki w UE wdrażające AI
(lub w zaawansowanym pilotażu)

2%

Systemy AI w UK z pełną autonomią
(reszta to wciąż asystenci).

+20 p.p.

Wzrost zautomatyzowanych
procesów w obsłudze klienta (NatWest).

£100 mln

Oczekiwany zysk z agentowej AI w 2026 roku
(Lloyds).

Jak badaliśmy rynek:

źródła, metoda i ograniczenia analizy

Ten dokument to pragmatyczna ocena transformacji europejskiego sektora finansowego w kierunku Agentic Banking w 2026 roku i w perspektywie na kolejne lata. Aby uzyskać możliwie najbardziej obiektywny obraz, zestawiliśmy 3 niezależne perspektywy.

1.1

Trzy filary analizy: regulacje, wdrożenia i koszty

Przeanalizowaliśmy dokumenty kluczowych instytucji nadzorczych takich jak EBA, ESMA, EBC, Bank of England oraz FCA. Pozwala to zrozumieć sztywne granice przepisów, które ograniczają rozwój technologii. Publikacja szczegółowo omawia wymogi wynikające z AI Act, PSD3, FIDA oraz PLD.

Zbadaliśmy faktyczne wdrożenia w tradycyjnych bankach takich jak Lloyds, NatWest, CaixaBank oraz ING. Przyjrzelśmy się również instytucjom finansowym typu fintech, w tym Revolut i N26. Publikacja uwzględnia dodatkowo infrastrukturę oferowaną przez Visa, Mastercard oraz Stripe.

Zestawiliśmy te obserwacje z analizami czołowych firm doradczych (Deloitte, McKinsey, BIS) oraz realnymi kosztami operacyjnymi i wydatkami na utrzymanie infrastruktury w chmurze i modeli LLM.

Wybrane źródła pozwalają zweryfikować rynkowy entuzjazm dotyczący sztucznej inteligencji i skupić się na rozwiązaniach faktycznie wykonalnych, opłacalnych oraz legalnych w ściśle regulowanym europejskim środowisku.

1.2

Ramy analizy: ograniczenia i założenia

Dla zachowania pełnej przejrzystości wskazujemy uwarunkowania, które wpływają na naszą ocenę:

1. Brak jednolitej nomenklatury: pojęcie Agentic Banking nie ma jeszcze ścisłej definicji prawnej (EBA posługuje się ostrożnym terminem „so called Agentic AI”). Rynek różnie klasyfikuje zaawansowane chatboty i faktyczne systemy oparte na agentach, co może zaburzać spójność statystyk.

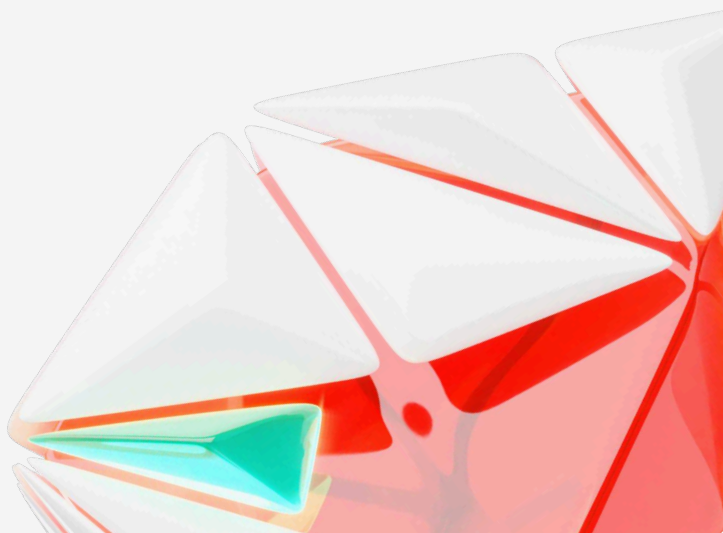
2. Ewoluuujące prawo: raport opiera się na obecnym stanie prawnym z 2026 roku i wybiega w przyszłość. Główne filary (jak AI Act) są już uchwalone, ale akty prawne i techniczne standardy klasyfikacji ryzyka podlegają częstym zmianom.
3. Bariery geograficzne: nasze wnioski dotyczące dopuszczalnej autonomii agentów AI dotyczą specyfiki ściśle regulowanego rynku europejskiego (UE i UK). Inicjatywy z USA czy Singapuru stanowią ciekawy punkt odniesienia, ale nie da się ich bezpośrednio przełożyć na grunt unijny ze względu na inne standardy ochrony danych (RODO) i wymogi dotyczące autoryzacji (PSD3).

1.3

Kluczowe wskaźniki (obraz rynku 2026+)

Zanim przejdziemy do szczegółów, oto wartości, które najlepiej ilustrują obecny etap rozwoju sztucznej inteligencji w bankowości:

- 92% unijnych banków już wdraża rozwiązania AI, a pozostałe 8% przygotowuje się do startu lub prowadzi zaawansowane testy wewnętrzne.
- 2% systemów AI w brytyjskich finansach działa w 100% samodzielnie. Niemal każda decyzja i akcja maszyny wciąż wymagają weryfikacji lub nadzoru człowieka.
- +20 p.p. wynosi odsetek całkowicie autonomicznie rozwiązywanych spraw przez Agentic Banking w obsłudze klienta na bazie 21 zoptymalizowanych procesów w NatWest.



Czym jest Agentic Banking

i na jakim etapie jest rynek?

W regulacjach europejskich nie istnieje dziś odrębna definicja Agentic Banking. EBA używa ostrożnego określenia „so called Agentic AI”, bacznie przyglądając się wdrożeniom AI w bankowości i płatnościach. Deloitte opisuje Agentic Banking jako systemy zdolne do samodzielnego rozumowania i wykonywania złożonych zadań w ramach wyznaczonych celów biznesowych, podczas gdy BIS wyraźnie rozróżnia asystentów AI – wspierających pracę człowieka – od systemów automatyzujących konkretne zadania i przez to częściowo zastępujących człowieka.

Agentic Banking to model bankowości, w którym sztuczna inteligencja wykracza poza odpowiadanie na pytania i formułowanie rekomendacji – potrafi samodzielnie realizować cele. AI rozumie potrzeby klienta lub pracownika, dzieli zadanie na poszczególne etapy, pobiera potrzebne dane, korzysta z narzędzi i systemów bankowych, proponuje kolejne działania, a w wybranych przypadkach, oczywiście w granicach zdefiniowanych uprawnień, samodzielnie podejmuje decyzje.

Warto tu wprowadzić proste rozróżnienie trzech modeli. Chatbot działa reaktywnie, odpowiadając na pytania. Klasyczny asystent AI, czyli copilot, rozumie już szerszy kontekst – potrafi wyszukiwać informacje, tworzyć streszczenia czy rekomendacje, a nawet przygotowywać kolejne kroki – ale to człowiek musi prowadzić cały proces. Agentic Banking zasadniczo różni się od obu tych modeli. Taki system samodzielnie planuje całą sekwencję działań, korzysta z wielu różnych narzędzi oraz źródeł danych, potrafi zareagować na nietypowe sytuacje i wykryć błędy lub odstępstwa od reguł. Jego nadrzędnym celem jest doprowadzenie sprawy klienta do końca - włącznie z wykonaniem potrzebnych działań i zamknięciem procesu.

Kluczowa zmiana dotyczy zakresu uprawnień systemu, który ewoluuje od wyjaśniania problemów i formułowania rekomendacji aż po przygotowanie oraz ostateczne wykonanie transakcji. Na najwyższych poziomach sprawczości system musi spełniać wymogi dyrektywy PSD2, w tym zasady silnego uwierzytelniania i uzyskania wyraźnej zgody klienta. W odpowiedzi na te wymagania operatorzy systemów płatności wdrażają nowe systemy delegacji uprawnień umożliwiające algorytmom działanie w imieniu użytkownika zgodnie z procedurami bezpieczeństwa.

Chatbot

Tylko odpowiada na pytania.
Akcję zawsze wykonuje człowiek.

Niska autonomia

**Copilot**

Analizuje dane i proponuje kroki. Człowiek musi kliknąć „zatwierdź”.

Średnia autonomia

**Agent AI**

Samodzielnie planuje i wykonuje operacje.
Działa w ramach nałożonych limitów.

Wysoka autonomia



Ewolucja AI (Chatbot vs Copilot vs Agent)

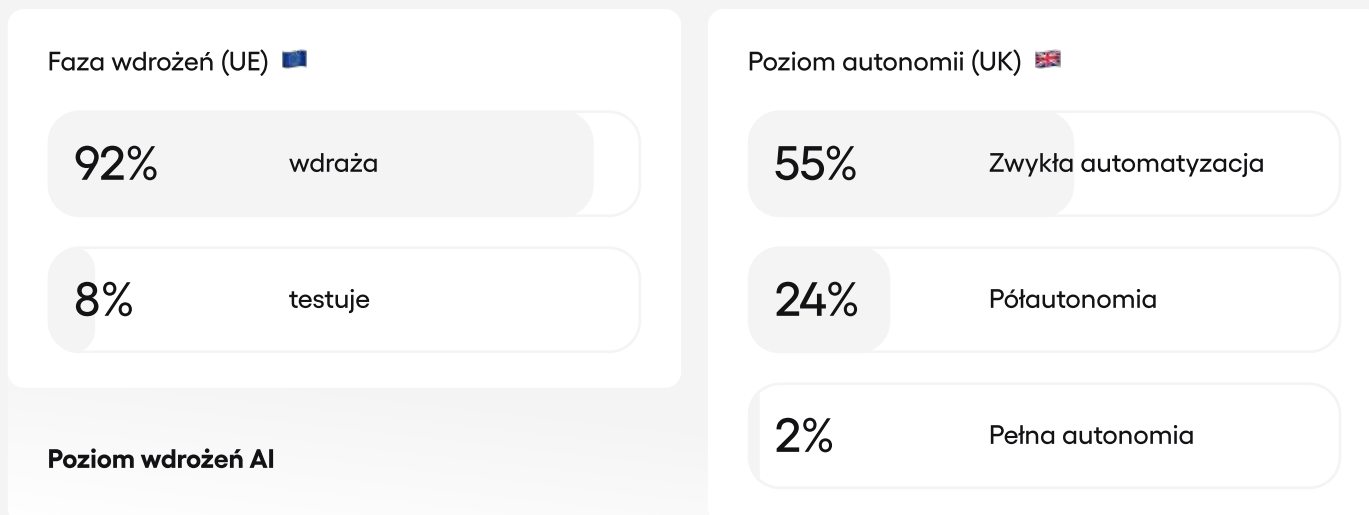
2.1

Powszechne wdrożenia, ale ograniczona autonomia – obraz rynku europejskiego

Wbrew powszechnemu przekonaniu Europa nie zaczyna od zera w obszarze Agentic Banking. EBA podaje, że 92% banków w UE już wdraża sztuczną inteligencję, a pozostałe 8% jest na etapie pilotażu lub wewnętrznych dyskusji. W bezpośredniej obsłudze klienta 55% badanych banków wykorzystuje modele generatywne lub rozwiązania agentowe, najczęściej w wykrywaniu i zgłaszaniu oszustw lub podejrzaney aktywności, wsparciu agentów i centrów obsługi telefonicznej, samoobsłudze klienta, narzędziach do edukacji finansowej oraz w cyfrowych asystentach i botach głosowych.

Brytyjski rynek przez wielu ekspertów uważany jest za lidera we wprowadzaniu innowacyjnych rozwiązań z zakresu Agentic Banking. Według Bank of England i FCA 55% systemów AI ma jakiś poziom automatyzacji decyzji, 24% z nich – charakter półautonomiczny, ale zaledwie 2% uznano za w pełni autonomiczne. Ten sam raport odśladnia też pewne ograniczenia. Otóż wiele instytucji tylko częściowo rozumie technologię AI, głównie ze względu na zależności od zewnętrznych dostawców modeli i danych oraz od infrastruktury w chmurze.

Mamy tu więc do czynienia z pozornie sprzecznymi wnioskami. Wdrożenia AI postępują szybko, ale tempo, w jakim rośnie rzeczywista autonomia systemów, pozostaje umiarkowane. Deloitte i McKinsey zgodnie wskazują, że dominują wciąż prostsze rozwiązania, a rzeczywista wartość pojawia się dopiero wtedy, gdy bank przeprojektuje sposób pracy od podstaw, zamiast mnożyć kolejne programy pilotażowe. Tam, gdzie to się udaje, potencjał jest znaczny.



2.2

Europa: co robią dziś banki i fintechy

1. Wielka Brytania jako lider wdrożeń Agentic Banking w obsłudze klienta

Tak jak wcześniej wspomnieliśmy, Wielka Brytania jest obecnie uważana przez wielu ekspertów za lidera wdrażania Agentic Banking w bankowości detalicznej. Lloyds Banking Group ogłosił uruchomienie pierwszego w UK asystenta finansowego opartego na AI, przeznaczonego dla 21 milionów użytkowników aplikacji mobilnej. Bank wyraźnie odróżnia ten produkt od tradycyjnych wirtualnych asystentów - ma on zapewniać spersonalizowane wsparcie i coaching finansowy, wykorzystywać systemy oparte na agentach do dzielenia zapytań klienta na mniejsze etapy i planowania działań. Lloyds podkreśla przy tym, jak ważne jest utrzymanie wysokich standardów w zakresie działania systemów AI, obejmujące m.in. skuteczne mechanizmy bezpieczeństwa oraz rozwiązywanie gwarantujące pełną wyjaśnialność.

Grupa podała, że rozwiązania AI wygenerowały około 50 milionów funtów w 2025 roku, a w 2026 oczekuje ponad 100 milionów funtów. W 2025 roku wdrożono ponad 50 systemów AI, a 2026 ma być rokiem skalowania Agentic Banking w całej organizacji.

Podobną ścieżką podąża NatWest, który we współpracy z OpenAI zapowiedział wykorzystanie AI do bardziej złożonych zadań - od identyfikacji oszustw i przeprowadzenia klienta przez cały proces reklamacji, po pomoc w rozumieniu sytuacji finansowej i planowaniu celów. W lutym 2026 roku bank podał, że 25 tysięcy klientów uzyska dostęp do nowego asystenta finansowego w systemie Cora.

W 2025 roku Cora obsłużyła 12,9 miliona zapytań dot. bankowości detalicznej, z czego połowa nie wymagała udziału człowieka. Wdrożenie Agentic Banking w 21 procesach obsługi klienta zwiększyło liczbę automatycznie rozwiązyanych spraw o 20 punktów procentowych.

To wyraźny wzrost skuteczności względem wyników osiągniętych wcześniej przy użyciu „klasycznego AI”. Wzrost skuteczności można powiązać z faktem, że AI rozumie kontekst pytania na tyle dobrze, by prowadzić klienta przez cały proces rozwiązywania problemu.

2. Unia Europejska i Polska

W UE CaixaBank uruchomił w aplikacji mobilnej agenta, który pomaga klientom porównywać produkty i karty, rekomendować najlepsze opcje, a w kolejnym etapie przeprowadzać klienta krok po kroku przez wniosek lub zakup. Bank jednocześnie informuje, że z rozwiązania skorzystało już 200 tysięcy klientów.

ING wdrożyło chatbota opartego na AI w sześciu rynkach, równolegle wykorzystuje sztuczną inteligencję do automatycznej oceny wniosków w finansach konsumenckich, a osobny moduł AI wykrywa nietypowe wzorce transakcyjne w procesach KYC.

Zamiast szukać pojedynczego mobilnego superasystenta, europejskie rynki stawiają na inne rozwiązanie. Agentic Banking w Unii Europejskiej tworzy sieć wyspecjalizowanych procesów oraz modeli.

Na polskim rynku wdrażanie rozwiązań AI w bankowości również nabiera tempa. PKO Bank Polski jest liderem – jego 17 voicebotów AI przeprowadziło łącznie ponad 70 milionów rozmów z klientami, a asystent głosowy w aplikacji IKO obsługuje 5,6 miliona użytkowników i rozumie 360 tematów konwersacyjnych. Wewnętrznie 11 tysięcy pracowników banku korzysta z wyszukiwarki AI, a 1400 programistów – z asystenta kodowania.

mBank wdrożył BOT-a Marek, czyli voicebota, który od maja 2025 roku dzwoni do klientów w celu weryfikacji podejrzanych transakcji. ING Bank Śląski z kolei uruchomił w grudniu 2025 roku pilotażowego asystenta AI opartego na GenAI dla klientów biznesowych – jest to pierwsza taka implementacja w grupie ING, a pełne wdrożenie planowane jest na początek 2026 roku. Polskie banki podchodzą do Agentic Banking ostrożnie, ale konsekwentnie – budując wewnętrzne kompetencje, szczególnie w obszarze obsługi klienta i wykrywania oszustw.

3. Fintechy – ostrożność przy doradztwie

Przykładem ostrożnego podejścia jest N26. Firma wdrożyła moduł inteligentnych analiz, który generuje spersonalizowane sugestie, jednak zastrzega, że mają one wyłącznie charakter informacyjny. Rekomendacje są oznaczane jako wygenerowane przez AI, a użytkownik może cofnąć zgodę na korzystanie z modułu.

Przykład Revolut jest kolejnym przykładem nieco zachowawczego podejścia - asystenci pomagają klientom rozumieć ofertę, analizować

wydatki i wspierać planowanie budżetu. Podobnie jak N26 firma zastrzega, że oferowane treści mają charakter wyłącznie informacyjny i nie stanowią porad inwestycyjnych, finansowych, podatkowych ani prawnych.

Użytkownik może też w każdej chwili przełączyć się na kontakt z ludzkim doradcą. Kluczowy etap stanowią jednak zmiany, które Revolut wprowadził bezpośrednio w systemie płatności. Revolut Pay jako jeden z pierwszych europejskich instrumentów finansowych zyskał pełną zgodność z brytyjskim oraz europejskim protokołem Google Agent Payments Protocol. Dzięki temu dynamiczne fintechy mogą wyprzedzić tradycyjne banki i szybciej opanować handlowy obszar obsługiwany przez Agentic Banking. To nie jest przypadkowy ruch, to jest przemyślana strategia wdrażania nowoczesnych usług przy jednoczesnym zachowaniu dużej ostrożności wobec autonomicznego doradztwa.

Fintechy mogą więc szybciej niż tradycyjne banki wejść w obszar handlu obsługiwanego przez Agentic Banking, nawet jeśli nadal ostrożnie podchodzą do „autonomicznego doradztwa”.

4. Nordea i Santander – co duże banki planują na kolejne lata?

Nordea podkreśla, że AI ma wzmacniać relację z klientem, uzupełniając pracę doradcy o szybszy dostęp do danych i analiz. Zaznacza też, że nadzór ludzki nadal będzie pełnił kluczową rolę.

Santander z kolei wspomina o skalowaniu rozwiązań AI i transformacji front office oraz back office, a w dalszej perspektywie podkreśla konieczność budowy bardziej konwersacyjnej bankowości.

Wielka Brytania (Lloyds, NatWest, Revolut)

Autonomiczna obsługa klienta
i zautomatyzowane płatności.

Hiszpania (CaixaBank, Santander):

Agenci zakupowi
i transformacja back-office.

Skandynawia (Nordea)

AI jako asystent ludzkiego
doradcy.

Niemcy (N26)

Analizy wydatków i coaching
finansowy.

Holandia (ING)

Detekcja
fraudów i automatyzacja AML.

2.3

JP Morgan, Wells Fargo i DBS – jak banki poza Europą wyprzedzają stary kontynent?

JP Morgan Chase jest jednym z najbardziej zaawansowanych banków na świecie w zakresie wdrażania AI. Bank uruchomił wewnętrznego asystenta LLM Suite, który w ciągu ośmiu miesięcy od premiery został udostępniony 200 tysiącom pracowników, a we wrześniu 2025 roku korzystało z niego już 250 tysięcy osób, z czego połowa deklaruje, że robi to codziennie. Budżet technologiczny JP Morgan wzrósł do niemal 20 miliardów dolarów w 2026 roku, a około 25% tych wydatków jest bezpośrednio powiązanych z AI.

Bank rozwija także rozwiązania agentowe w płatnościach – we współpracy z Mirakl uruchomił platformę Agentic Commerce, w której agenci AI dokonują zakupów w imieniu konsumentów.

Wells Fargo z kolei wdrożył asystenta Fargo opartego na AI, który w 2024 roku obsłużył ponad 245 milionów interakcji z klientami – ponad dwukrotnie więcej niż prognozowano. Architektura Fargo działa w modelu zero-PIL, co oznacza, że żadne dane osobowe nie trafiają do modelu językowego. W sierpniu 2025 roku Wells Fargo rozszerzył współpracę z Google Cloud i wdrożył platformę Google Agentspace dla 215 tysięcy pracowników, wprowadzając agentów AI do oddziałów, bankowości inwestycyjnej i centrów obsługi.

Bank of America podaje, że asystentka Erica odnotowała ponad 2,5 miliarda interakcji z użytkownikami - aktywnie korzysta z niej 20 milionów osób. Erica zarządza subskrypcjami, analizuje wydatki oraz wyszukuje numery rozliczeniowe i transakcje. Obsługuje też przelewy i płatności.

Warto zaznaczyć, że bank nadal korzysta z ludzkiego nadzoru, gdyż złożone sprawy ostatecznie przejmuje pracownik. To przykład skutecznej, ale nie w pełni autonomicznej bankowości.

Z kolei DBS w Singapurze wdrożył model przeznaczony dla bankowości korporacyjnej. Chatbot DBS Joy, oparty na AI, zapewnia klientom firmowym całodobowy dostęp do wirtualnego wsparcia, a w trudniejszych sprawach łączy ich z ekspertem, który dodatkowo otrzymuje pomoc inteligentnego asystenta.

Od rozpoczęcia testów do listopada 2025 roku Joy obsłużył przeszło 120 tysięcy czatów. Z rozwiązania tego korzysta około 4 tysięcy firmowych klientów miesięcznie. Bank wdrożył ponad 1500 modeli AI, które obsługują przeszło 370 procesów. W 2025 roku przyniosło to powyżej 1 miliarda dolarów singapurskich zysku.

Równie szybko Agentic Banking rozwija się w wewnętrznych procesach. Australijski CommBank w ramach projektu Coral łączy narzędzia do monitoringu z analizą kodu. System samodzielnie przygotowuje zapytania o zmiany oraz proponuje poprawki, chociaż to inżynierowie muszą ostatecznie zatwierdzić każdą modyfikację.

Najważniejsze wnioski



Agentic Banking nie tylko odpowiada na pytania (jak chatbot), ale sam planuje i realizuje procesy od początku do końca.



Liderem dużych wdrożeń w Europie jest Wielka Brytania (szczególnie Lloyds i NatWest).



Banki na kontynencie i fintechy (Revolut, N26) stawiają na analizę danych i celowo unikają w pełni autonomicznego doradztwa.



Agentic Banking to już nie ciekawostka technologiczna, ale fundament zmiany całej organizacji.



Granice prawne i regulacyjne

3.1

Regulacje w Europie – AI Act

Rozwój Agentic Banking w UE zależy od zgodności z restrykcyjnymi regulacjami i standardami technicznymi. Wyniki wdrożeń w 2026 roku będą uwarunkowane dostosowaniem systemów do unijnych przepisów dotyczących ochrony konsumentów i stabilności rynków finansowych.

Europejski akt w sprawie sztucznej inteligencji (AI Act)

Aktem prawnym kształtującym cały ten ekosystem jest Europejski Akt w sprawie Sztucznej Inteligencji (Regulation EU 2024/1689), który wszedł w życie w sierpniu 2024 roku. Przepisy rozporządzenia wprowadzane są kaskadowo, a regulacje o istotnym znaczeniu dla sektora finansowego zaczną w pełni obowiązywać od 2 sierpnia 2026 roku - z wyjątkiem wybranych przepisów dotyczących systemów wbudowanych jako komponenty bezpieczeństwa, których wprowadzenie zostało odłożone na 2027 rok.

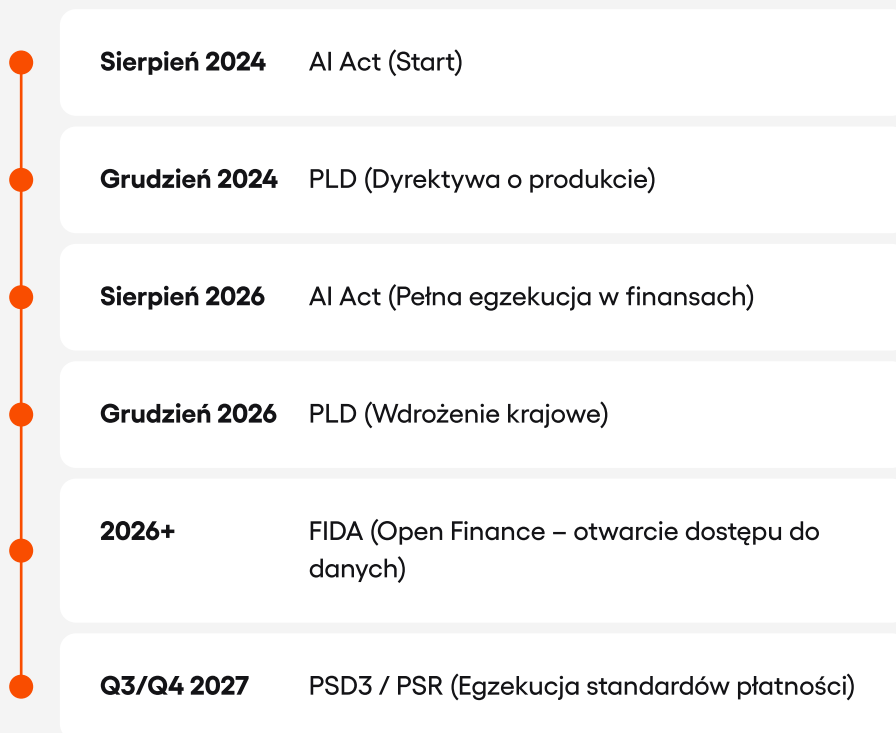
Dla instytucji bankowych najbardziej istotne znaczenie ma klasyfikacja systemów oparta na ryzyku, a w szczególności kategoryzacja ujęta w Załączniku III. Zgodnie z tymi przepisami systemy sztucznej inteligencji wykorzystywane do oceny zdolności kredytowej osób fizycznych lub do ustalania scoringu kredytowego są klasyfikowane jako systemy wysokiego ryzyka.

Taka klasyfikacja nakłada na banki i dostawców szereg obowiązków technicznych. Największym wyzwaniem dla pełnej automatyzacji jest wymóg zapewnienia skutecznego nadzoru ludzkiego. Do 2 lutego 2026 roku Komisja Europejska została zobligowana do opublikowania szczegółowych wytycznych określających praktyczne wdrożenie zasad klasyfikacji wysokiego ryzyka.

Europejski Bank Centralny lobbował za zmianą definicji oraz zakresu klasyfikacji wysokiego ryzyka. Instytucja ta dążyła do wyłączenia z tej kategorii tradycyjnych modeli statystycznych. Propozycja dotyczyła uogólnionych liniowych modeli, takich jak logistyczna lub

liniowa regresja, które banki powszechnie stosują w ocenie kredytowego ryzyka.

Argumentacja EBC opiera się na założeniu, że te modele, w przeciwieństwie do głębokich sieci neuronowych, charakteryzują się wysokim poziomem wyjaśnialności i przejrzystości.



Jak EBA i ESMA dopasowują AI Act do istniejących przepisów finansowych

W 2025 roku europejska EBA dogłębnie przeanalizowała rynkowe powiązania między unijnym AI Act a finansowymi przepisami w celu uniknięcia nakładania nowych obowiązków na istniejące zasady. Przeprowadzona analiza szczegółowo objęła wzajemne relacje pomiędzy CRD, CRR, PSD2, PSD3 wymogami DORA oraz innymi sektorowymi regulacjami. Europejski regulator uznał, że wszystkie wymienione akty są w pełni komplementarne.

Wdrożenie Agentive Banking polega na włączeniu inteligentnych algorytmów w struktury zarządzania operacyjnym oraz technologicznym ryzykiem. Taka integracja sprawia, że tworzenie osobnych kontrolnych departamentów staje się zbędne. W latach 2026 i 2027 EBA ujednolici sposób sprawowania nadzoru przez krajowe organy.

Równolegle ESMA zaostrzyła kontrolę w obszarze inwestycyjnych usług oraz kapitałowych rynków. Narzędzia stosowane w doradztwie, wykrywaniu oszustw oraz obsłudze klienta podlegają unijnej dyrektywie MiFID II. W 2026 roku zaktualizowano wytyczne i włączono algorytmy do rynkowych zasad.

Instytucje finansowe muszą zachować staranność pomimo postępującej automatyzacji. Wymagane jest zapobieganie dyskryminacji oraz zapewnienie jakości danych. Pracownicy powinni unikać bezkrytycznego akceptowania rekomendacji generowanych przez system.

3.2

Kto odpowiada za błędy AI – dyrektywy PLD, AILD i koncepcja cyfrowego powiernika

Wdrażanie autonomicznych rozwiązań do zawierania umów oraz inicjowania nieodwracalnych płatności zmienia podejście do prawa zobowiązań. Systemy te samodzielnie zarządzają portfelami inwestycyjnymi, co wymusza aktualizację przepisów dotyczących czynów niedozwolonych. Tradycyjne regulacje muszą uwzględniać mechanizmy automatycznego generowania oświadczeń woli.

Obecnie europejskie sądy, działy prawne oraz organy regulacyjne analizują zjawisko luki w odpowiedzialności. Wynika ona z natury systemów AI, które działają w sposób probabilistyczny oraz ewolucyjny. Skutków ich operacji nie przewidzi użytkownik ani projektant. Unijna odpowiedź na te problemy opiera się na dwóch konkretnych rozwiązaniach prawnych.

Zrewidowana dyrektywa o odpowiedzialności za produkty wadliwe (PLD)

Głównie zrewidowana Dyrektywa w sprawie odpowiedzialności za produkty wadliwe (Product Liability Directive, PLD 2024/2853), po wejściu w życie w grudniu 2024 roku, nakłada na państwa członkowskie obowiązek wdrożenia przepisów do prawa krajowego najpóźniej do 9 grudnia 2026 roku. Z punktu widzenia technologii Agentic Banking jest to akt wyjątkowy - po raz pierwszy jednoznacznie rozszerza definicję „produktu” na oprogramowanie, w tym na zaawansowane systemy sztucznej inteligencji.

Zrewidowana PLD opiera się na modelu odpowiedzialności na zasadzie ryzyka. Poszkodowany - na przykład klient banku, którego system AI zawarł wyjątkowo niekorzystną umowę w wyniku niezamierzonego działania - nie musi udowadniać po stronie banku niedbalstwa ani braku staranności. Wystarczy dowód, że system AI był „wadliwy”, oraz wykazanie samej szkody. Jeśli algorytm negocjuje w imieniu klienta warunki lokaty, ale wskutek błędów w modelu zatwierdza produkt o znacznie gorszych warunkach, klient nie musi udowadniać, że bank zaniedbał testowanie modelu - wystarczy, że wykaże wadliwość systemu i poniesioną szkodę.

Przewidując, że poszkodowani konsumenci dysponują nieporównywalnie mniejszą wiedzą na temat budowy modeli typu czarna skrzynka niż korporacje finansowe, prawodawca wprowadził istotne ułatwienie procesowe: domniemanie związku przyczynowego w przypadku

technologii o wysokim stopniu skomplikowania. Bank wdrażający rozwiązanie z obszaru Agent Banking staje się bezpośrednio narażony na roszczenia, nawet gdy błędne działanie wynika z pomyłek w modelu AI. Ponieważ sądy konsekwentnie odrzucają koncepcję przyznania sztucznej inteligencji jakiegokolwiek osobowości prawnej, pełny ciężar odpowiedzialności materialnej spoczywa na podmiocie komercyjnym kontrolującym środowisko wdrożeniowe.

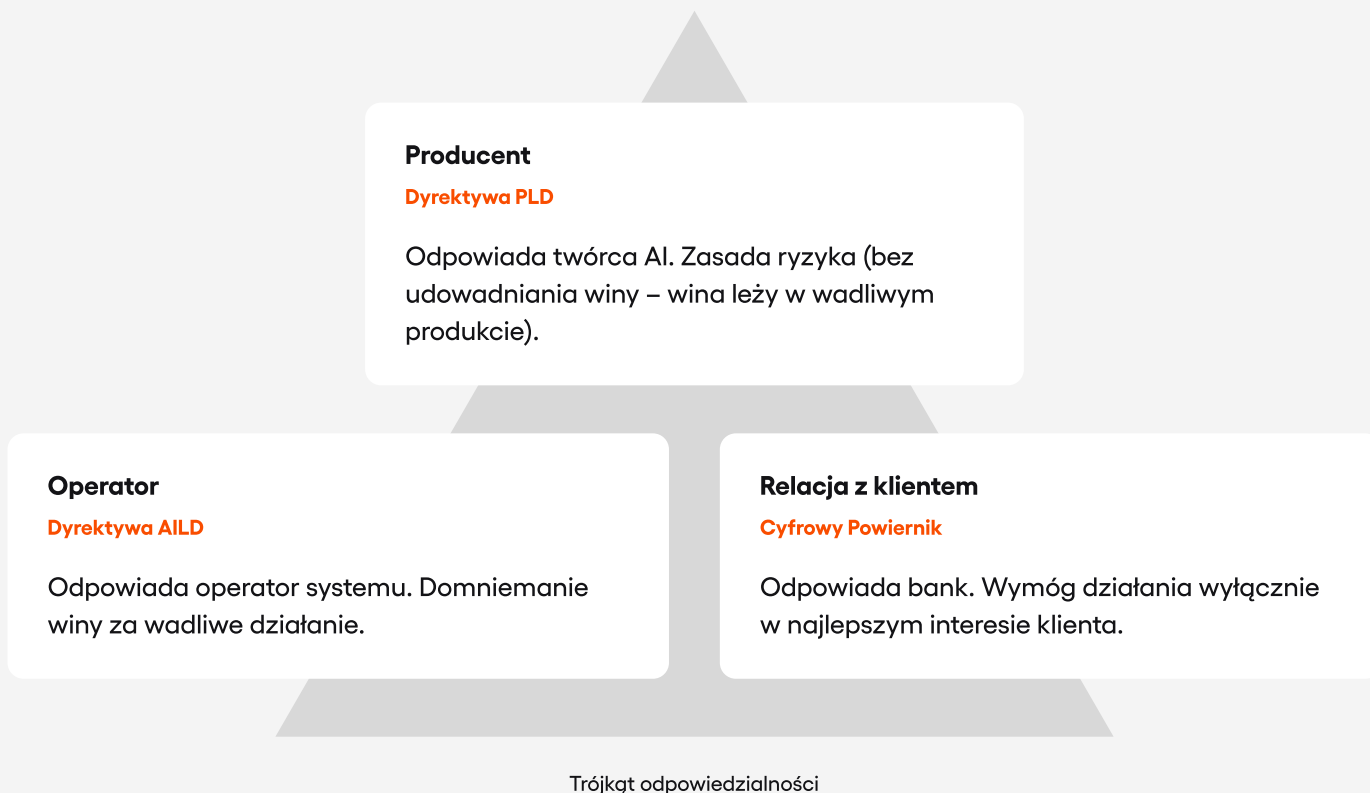
Dyrektywa o odpowiedzialności za sztuczną inteligencję (AILD) i cyfrowy powiernik

PLD pokrywa szkody wynikające z „wadliwości” samego produktu, ale otwarta pozostaje kwestia dochodzenia odszkodowań na zasadach winy za szkody wyrządzone przez działania wspierane przez AI, które niekoniecznie wynikają z samej „wady” kodu, lecz z błędnego zastosowania lub niewystarczającego nadzoru nad algorytmem. W tym celu powstała dyrektywa o odpowiedzialności za sztuczną inteligencję (AILD). Wprowadza zasadę domniemania winy oraz obowiązek ujawniania dokumentacji algorytmów przez operatorów. Takie rozwiązanie ułatwia dochodzenie roszczeń, ponieważ to firma musi udowodnić, że system zadziałał poprawnie.

Na początku 2026 roku prace nad dyrektywą AILD zostały wstrzymane. Komisja Europejska rozważa wycofanie wniosku z powodu braku politycznego porozumienia. Taki impas prowadzi do powstania luki prawnej. Jeśli dyrektywa upadnie, poszkodowani będą musieli korzystać z przestarzałych przepisów krajowych poszczególnych państw unijnych.

W efekcie branża finansowa proponuje koncepcję Cyfrowego Powiernika. Zakłada, że banki udostępniające autonomiczne systemy doradcze mają dwa główne obowiązki. Pierwszy to staranność, która wymusza, by system działał co najmniej tak dobrze jak ludzki doradca. Drugi to lojalność, wymagająca od algorytmu dbania wyłącznie o interes konsumenta bez promowania produktów banku.

W praktyce oznacza to wprowadzanie do umów z dostawcami chmury konkretnych kar. Zapisy przenoszą odpowiedzialność finansową za błędy AI oraz wycieki danych na dostawcę technologii. Obejmują również sytuacje, w których system zawiera umowę w imieniu klienta bez jego zgody.



3.3

Otwarte finanse (Open Finance) – siła napędowa rozwoju technologii poprzez PSD3 i FIDA

Rozwój zaawansowanych ekosystemów sztucznej inteligencji opartej na Agentlic Banking w sektorze finansowym nie byłby możliwy bez równoczesnej, głębokiej przebudowy infrastruktury udostępniania i przetwarzania danych. Systemy AI z definicji potrzebują dostępu do danych w czasie rzeczywistym - bez nich pozostają zaledwie zaawansowanymi algorytmami wykorzystywanymi do konwersacji.

Nowy pakiet przepisów Unii Europejskiej zmienia u podstaw model wymiany informacji finansowych, przesuwając ciężar z ograniczonej koncepcji „Open Banking” na całościową „Open Finance”.

PSD3 i PSR. Ewolucja ram płatniczych

W listopadzie 2025 roku, po wielomiesięcznych negocjacjach, Parlament Europejski i Rada UE osiągnęły porozumienie polityczne w sprawie ostatecznego kształtu Trzeciej Dyrektywy w sprawie Usług Płatniczych (PSD3) oraz nowego, bezpośrednio wiążącego Rozporządzenia w sprawie Usług Płatniczych (PSR). Oba akty prawne wejdą w życie prawdopodobnie w 2026 roku, ale z uwagi na założony 18- do 21-miesięczny okres przejściowy na wdrożenie techniczne, pełne egzekwowanie nowych norm na rynku nastąpi najwcześniej w drugiej połowie 2027 roku.

Przepisy te gruntownie przebudowują środowisko dla usług inicjowania płatności i usług dostępu do informacji o rachunku. PSR koncentruje się na

znacznym ulepszeniu protokołów silnego uwierzytelniania klienta (SCA), wprowadzeniu wymogów dotyczących przejrzystości, bezwarunkowego dostępu do systemów płatności dla niebankowych dostawców usług - takich jak instytucje pieniądza elektronicznego - a przede wszystkim na zastrzeżeniu odpowiedzialności podmiotów płatniczych za oszustwa.

Oznacza to, że infrastruktura, po której poruszać się będą inteligentne rozwiązania płatności klienckich, będzie znacznie głębiej zintegrowana, z API, co zminimalizuje niespójności przepisów i umożliwi dostawcom oferowanie usług transgranicznych bez technicznych barier.

FIDA (Financial Data Access). Fundament informacyjny dla Agentic Banking

Podczas gdy PSD3 usprawnia infrastrukturę płatniczą FIDA zapewnia systemom AI niezbędne dane operacyjne, czyli kompleksową wiedzę o konsumencie. FIDA, będąca kamieniem węgielnym Europejskiej Strategii Finansów Cyfrowych, dokonuje dużego kroku: rozszerza zasady udostępniania danych zorientowane na rachunki płatnicze, znane z PSD2, na cały przekrój produktów sektora finansowego. Na wyraźne żądanie i w oparciu o zgodę klienta instytucje będą musiały za pośrednictwem ustandaryzowanych API otwierać dostęp do danych dotyczących ubezpieczeń, funduszy emerytalnych, kredytów hipotecznych, a w przyszłości także portfeli kryptoaktywów.

Rozporządzenie to formalizuje nową kategorię uczestników rynku: Dostawców Usług Informacji Finansowej, którzy będą głównymi operatorami zaawansowanych rozwiązań AI. System dysponujący pełnym profilem klienta uzyska zdolność do autonomicznego modelowania i optymalizowania finansów - zamiast ograniczać się do raportowania historii przelewów, wykorzysta dyrektywę FIDA, aby zidentyfikować niekorzystne polisy ubezpieczeniowe i automatycznie obliczyć, ile klient zyska na zerwaniu lokaty na rzecz atrakcyjniejszego funduszu. W następnym kroku mógłby wynegocjować warunki i zrealizować transfer kapitału w ułamku sekundy, zwalniając konsumenta z konieczności samodzielnej analizy.

Taka transparentność i natychmiastowa mobilność danych budzą obawy tradycyjnych instytucji o utratę relacji z klientem na rzecz algorytmów analitycznych oraz interfejsów technologicznych dostarczanych przez podmioty BigTech.

RODO i SCHUFA. Problem nie kończy się na „skuteczności modelu”

Kolejną istotną granicę wyznaczają przepisy RODO, zwłaszcza w zakresie zautomatyzowanego podejmowania decyzji oraz profilowania. EDPB podtrzymuje dotychczasowe wytyczne w tym obszarze. Wyrok Trybunału Sprawiedliwości UE w sprawie SCHUFA dowiódł, że automatyczne wygenerowanie oceny punktowej przez biuro kredytowe stanowi zautomatyzowaną decyzję indywidualną. Dzieje się tak pod warunkiem, że bank przypisuje temu wynikowi rolę decydującą przy przyznawaniu kredytu.

Problem wykracza poza samą jakość modelu. Kluczowe znaczenie ma to, czy człowiek faktycznie analizuje sprawę, czy jedynie formalnie podpisuje rozstrzygnięcie wygenerowane przez system. Jeśli analityk kredytowy otrzymuje od AI kompletną rekomendację i tylko ją zatwierdza, to w rzeczywistości decyzję podejmuje maszyna. W takim scenariuszu człowiek jedynie potwierdza gotowy wynik.

Dlatego w 2026 roku systemy AI przygotowujące analizę kredytową są rozwiązaniami możliwymi do wdrożenia. Znacznie trudniej jednak wprowadzić proces, w którym algorytm samodzielnie przyznaje kredyt detaliczny.

MiFID II i zarządzanie majątkiem. AI pod warunkiem zgodności z profilem i najlepszym interesem klienta

ESMA przypomina, że firmy wykorzystujące AI w usługach inwestycyjnych dla klientów detalicznych nadal muszą spełniać wymogi MiFID II. Te przepisy wymuszają dbanie o najlepszy interes klienta oraz zachowanie odpowiednich zasad działalności. Właśnie dlatego ESMA wskazuje konkretne sytuacje, w których można użyć AI. Algorytmy mogą wspierać obsługę klienta, wykrywać oszustwa, zarządzać ryzykiem oraz pomagać w doradztwie inwestycyjnym. Takie wyliczenie nie daje jednak zgody na wydawanie nieprzejrzystych rekomendacji generowanych przez AI.

Regulacja ta tłumaczy opisaną wcześniej ostrożność fintechów. Zastrzeżenia N26 oraz Revolut o informacyjnym charakterze produktów AI wynikają bezpośrednio z wymogów MiFID II. Rynek pokazuje, że zarządzanie majątkiem oraz doradztwo dopuszczają rozwiązania Agentlic Banking. Takie wdrożenia wymagają jednak pełnej przejrzystości oraz AI governance, co zapewnia ciągłą zgodność rekomendacji z profilem klienta.

Najważniejsze wnioski



AI Act traktuje algorytmy oceniające zdolność kredytową jako systemy wysokiego ryzyka.



Zgodnie z dyrektywą PLD banki i twórcy oprogramowania odpowiadają za błędy AI na zasadzie ryzyka.



Rozwój Agentic Banking zależy wprost od dyrektyw PSD3 i FIDA, które dają algorytmom dostęp do danych.



RODO wciąż mocno ogranicza sytuacje, w których maszyna sama podejmuje decyzję tylko na podstawie profilowania.



Technologia i koszty

– co napędza,
a co blokuje wdrożenia?

4.1

Dlaczego Agentic Banking wymaga przebudowy bankowego zaplecza IT?

Wprowadzenie inteligentnych modeli do architektury finansowej zmusza banki do przebudowy zaplecza technologicznego. Zmiana ta oznacza coś więcej niż zakup nowej warstwy oprogramowania. Agentic Banking wymaga zapewnienia odpowiedniej mocy obliczeniowej oraz bezpieczeństwa danych. Banki muszą jednocześnie kontrolować wydatki na operacje AI i łączyć nowoczesne narzędzia z systemami, które mają po dwadzieścia i więcej lat.

4.2

Partnerstwa chmurowe i nadzór ICT w świetle DORA

Przetwarzanie zapytań przez modele językowe oraz obsługa wielu procesów wymagają dużej i skalowalnej mocy obliczeniowej. Potrzebne są do tego zarówno procesory główne, jak i karty graficzne. Takie zapotrzebowanie tłumaczy, dlaczego niemal wszystkie banki decydują się na partnerstwa strategiczne oraz outsourcing systemów AI do chmury. Instytucje korzystają z usług największych dostawców na rynku, czyli AWS, Microsoft Azure oraz Google Cloud.

Dostawcy chmury podlegają ścisłej kategoryzacji jako krytyczni dostawcy usług zewnętrznych ICT (CTPPs), co wynika bezpośrednio z przepisów rozporządzenia DORA. Taka kwalifikacja pozwala organom nadzoru kontrolować ryzyko koncentracji operacyjnej, na które wskazują Europejski Bank Centralny oraz EBA. Uzależnienie niemal całego sektora od kilku gigantów technologicznych zagraża bowiem stabilności całego systemu finansowego.

Właśnie dlatego organy nadzoru, takie jak niemiecki BaFin, wymagają od banków wdrażania rygorystycznego AI governance w projektach chmurowych. Architektura systemów musi zapewniać dostępność zapisaną w umowach SLA oraz umożliwiać cykliczne testy odporności i penetracji (TLPT). Banki potrzebują również sprawdzonych planów awaryjnych. Takie procedury pozwalają szybko przenieść systemy na własne serwery, jeśli zewnętrzny dostawca zawiedzie. Dzięki temu bank zachowuje ciągłość działania swoich usług.

4.3

Architektura ochrony danych w środowiskach wieloagentowych

Banki wykorzystują architekturę RAG, aby zasilać wyizolowane modele AI wewnętrznymi procedurami oraz danymi klientów w czasie rzeczywistym. Takie rozwiązanie stwarza jednak wysokie ryzyko wycieku informacji objętych tajemnicą bankową. W konsekwencji błędy w tym procesie prowadzą bezpośrednio do naruszenia przepisów RODO.

W systemach Agentic Banking - gdzie jeden algorytm na przykład kategoryzuje zapytanie klienta, a drugi pobiera dla niego rekomendację giełdową - wyciek kontekstu i uprawnień, znany jako Capability Bleed, staje się jednym z największych wyzwań inżynierskich.

Jeśli proces odpowiedzialny za rekomendacje inwestycyjne uzyskuje nieintencjonalny dostęp do danych z modułu KYC, na przykład informacji o dochodach czy historii kredytowej, taki wyciek kontekstu mógłby prowadzić do naruszenia tajemnicy bankowej i łamania zasady minimalizacji danych z RODO.

Bezpieczeństwo danych wymaga, aby modele AI nie miały bezpośredniego dostępu do całych baz danych. Właśnie dlatego systemy muszą opierać się na rygorystycznej kontroli uprawnień (RBAC), konfigurowanej bezpośrednio w mechanizmach sterujących funkcjami zewnętrznymi.

Dodatkowo dane przesyłane do modelu muszą przechodzić przez filtry usuwające informacje pozwalające na identyfikację konkretnych osób. Takie zabezpieczenie chroni przed atakiem typu memory poisoning. Dzięki temu poufne dane klientów nie zostaną na stałe zapamiętane przez model AI, co zapobiega ich wyciekowi w razie włamania do systemu.

4.4

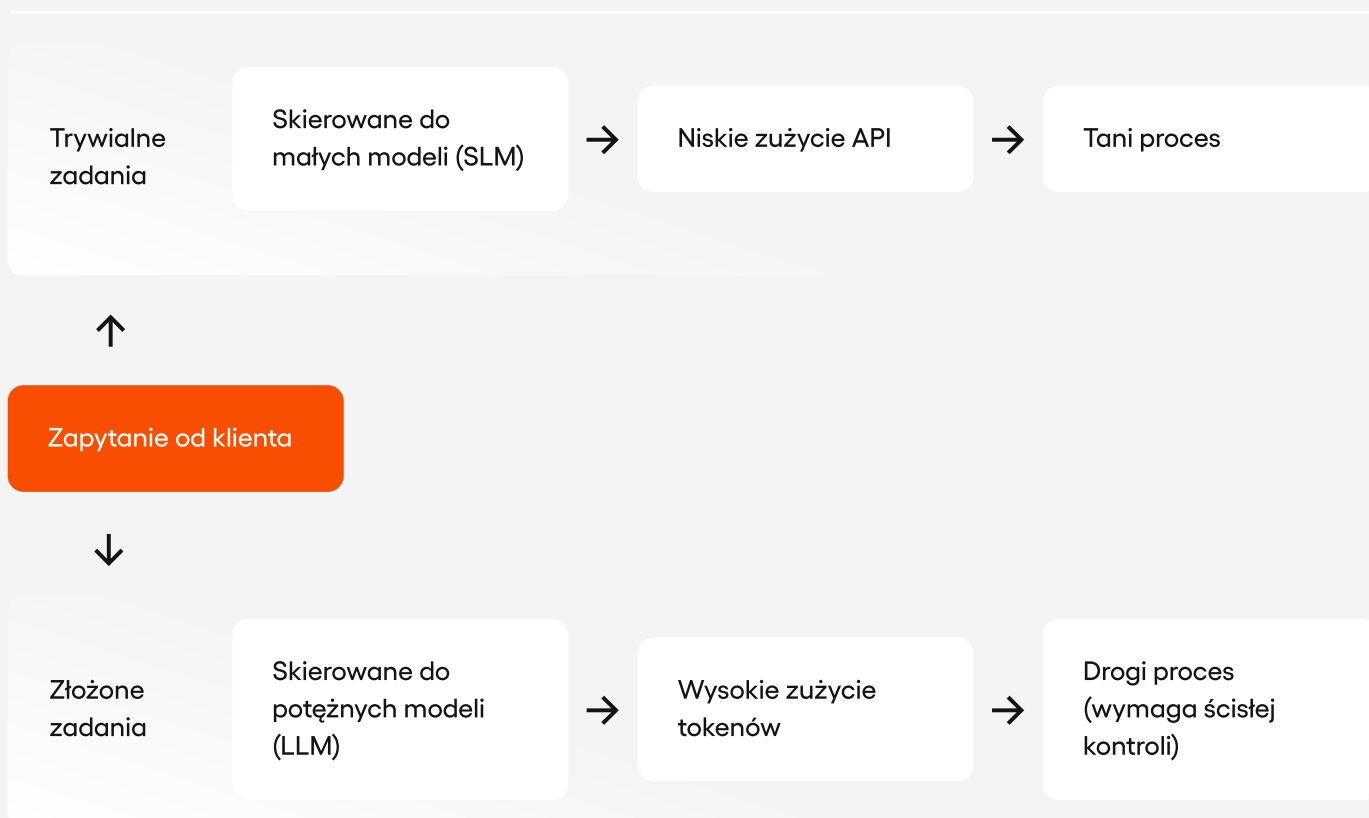
Ile kosztuje agent AI – strategie obniżania kosztów

Tradycyjne platformy SaaS do obsługi klienta charakteryzują się stabilnym modelem subskrypcyjnym, w którym opłata naliczana jest za każdego użytkownika (per seat), natomiast ekonomika jednostkowa technologii Agentic Banking jest definiowana zupełnie inaczej - niemal w 100% przez koszt przetwarzania tokenów przez natywne API modeli językowych.

Wydatki te rosną bardzo szybko, ponieważ autonomiczny system bankowy nie wykonuje jednej operacji, tylko przeprowadza wielostopniową analizę. Algorytm sprawdza błędy, weryfikuje warunki i powtarza cykle wnioskowania, co z każdym krokiem zwiększa ilość przesyłanych danych. Taki proces błyskawicznie podbija koszt obsługi pojedynczej transakcji lub rozmowy. Sytuację pogarszają dodatkowo nagłe zmiany cenników u dostawców LLM, co destabilizuje budżety projektów opartych wyłącznie na zewnętrznym API.

Właśnie dlatego europejskie banki wdrażają inteligentne kierowanie zapytań (Agent Mesh Topology). Proste operacje trafiają do mniejszych, otwartych modeli, a drogie i potężne narzędzia są uruchamiane tylko do trudnych analiz i końcowej weryfikacji. Dokładne liczenie tych ukrytych opłat bezpośrednio decyduje o tym, czy całe przedsięwzięcie będzie zarabiać.

Architektura kosztów (Agent Mesh)



4.5

Przestarzałe systemy Core Banking jako główna bariera integracji z AI

Przestarzała architektura IT to w Europie krytyczna przeszkoda. Główne systemy wielu banków (Core Banking) powstały jeszcze w latach 90. lub na początku obecnego milenium. Takie rozwiązania opierają się na sztywnych, monolitycznych strukturach, które bardzo trudno modyfikować. Ze względu na bezpieczeństwo ogromnej bazy klientów każda zmiana wiąże się z wysokim ryzykiem, więc banki za wszelką cenę unikają głębokiej modernizacji.

Tymczasem modele LLM działają zupełnie inaczej – wywołują funkcje przez nowoczesne standardy API. Tradycyjne, ociążone systemy rzadko pozwalają na taką sprawną komunikację. Ta luka zmusza instytucje do przebudowy infrastruktury i przejścia na elastyczne rozwiązania w chmurze.

W praktyce oznacza to oddzielenie samych operacji bankowych od zwinnych warstw komunikacyjnych, które łączą nowoczesne magistrale danych. Bez tej zmiany Agentic Banking pozostaje bezużyteczny – nie sprawdzi limitu na koncie ani nie pobierze danych klienta w ustandaryzowanym formacie.

Najważniejsze wnioski



Agentic Banking opiera się na chmurze, co silnie uzależnia rynek od zaledwie kilku wielkich dostawców technologii.



Współpraca wielu modeli AI rodzi ryzyko, że wrażliwe dane wyciekną z jednego procesu do drugiego.



Ze względu na rosnące koszty API, banki tną wydatki, kierując proste zadania do tańszych modeli (Agent Mesh).



Główne systemy bankowe są przestarzałe i blokują pełen potencjał nowych technologii.



Nowe protokoły płatnicze

– jak Visa, Mastercard i Stripe budują infrastrukturę dla agentów?

5.1

Wyścig o standard – protokoły autoryzacji płatności

Masowe wdrożenie Agentic Banking wymagało stworzenia uniwersalnych i wysoce zabezpieczonych protokołów maszynowych, zdolnych do bezpiecznego przenoszenia wrażliwych danych płatniczych oraz intencji zakupowych w środowisku sieciowym pełnym zagrożeń. Rok 2025 i początek 2026 przyniosły falę ogłoszeń od największych światowych graczy, rywalizujących o ustanowienie globalnych standardów autoryzacji dla sztucznej inteligencji.

Tabela protokołów płatniczych



Visa TAP

Weryfikacja tożsamości agenta na poziomie sieci (CDN/Edge).



Mastercard Agent Pay

Tokeny z zaszytymi na stałe regułami biznesowymi i limitami.



Stripe ACP

Uprawnienia przydzielane przez sklep (limit kwoty i czasu operacji).



Google AP2

Wieloetapowe mikrokontrakty (oddzielna zgoda na koszt, oddzielna na płatność).

Visa Trusted Agent Protocol (TAP)

Rozwiązanie zaprezentowane przez Visa, znane jako Trusted Agent Protocol (TAP), koncentruje się na dostarczeniu bezpiecznej infrastruktury umożliwiającej weryfikację intencji i tożsamości narzędzi AI bezpośrednio na warstwie protokołu HTTP - minimalizując konieczność wdrażania głębokich i kosztownych zmian w kodzie źródłowym sklepów internetowych. TAP opiera się na architekturze kryptograficznej wykorzystującej podpisy cyfrowe z infrastrukturą kluczy publicznych.

Mechanizm zaufania w TAP opiera się na kilku powiązanych elementach weryfikacji, które znajdują się w nagłówkach i treści zapytań API. Fundamentem jest sygnatura rozpoznawania. Ten unikalny identyfikator potwierdza, że system kontaktujący się z serwerem sprzedawcy to autoryzowany i zarejestrowany proces handlowy. Dzięki temu algorytm nie jest brany za bota zbierającego dane, co chroni przed blokadą przez zapory sieciowe WAF.

Drugi element stanowi kryptograficzne rozpoznawanie klienta. Moduł ten przekazuje sprzedawcy bezpieczny token (często jako JSON Web Token), który zawiera anonimowe dane o urzędzeniu, lokalizacji czy programie lojalnościowym. Całość uzupełnia weryfikacja klucza publicznego zapisanego jako zmienna kid.

Ostatnią warstwę tworzą zabezpieczone dane płatnicze. Jeśli system realizuje płatność, przesyła wygenerowany skrót kryptograficzny (hash) oraz niezbędne informacje, takie jak adres wysyłki i dane rozliczeniowe. Pozwala to sfinalizować transakcję bez pokazywania pełnego numeru karty (PAN) w oknie modelu językowego, co zapobiega wyciekowi danych.

Współpraca z firmami takimi jak Akamai czy Cloudflare pozwala weryfikować zapytania już na obrzeżach sieci (Edge). Dzięki temu systemy sprawdzają wiarygodność sygnatury bezpośrednio w węzłach CDN. Takie rozwiązanie pozwala błyskawicznie odrzucać próby ataku, zanim szkodliwe dane w ogóle zbliżą się do infrastruktury banku.

Mastercard Agent Pay i architektura Web Bot Auth

Mastercard rozwija platformę Agent Pay Acceptance Framework. Rozwiązanie gwarantuje jednoznaczną identyfikację każdego systemu AI dokonującego płatności, dzięki czemu każda transakcja jest autoryzowana oraz możliwa do prześledzenia. Platforma wykorzystuje standard uwierzytelniania Web Bot Auth (zgodny z IETF RFC 9421). Pozwala to sprzedawcom odróżnić zaufany algorytm od złośliwego bota jeszcze przed realizacją płatności.

Kluczowym elementem Agent Pay są dynamiczne tokeny płatnicze generowane w ramach ekosystemu Mastercard Digital Enablement Service (MDES). W odróżnieniu od tradycyjnych danych kartowych, tokeny

te mają wbudowane reguły bezpieczeństwa – na przykład pozwalają na płatność wyłącznie u konkretnego sprzedawcy, w określonym czasie i do ustalonego limitu kwotowego. Dzięki temu nawet jeśli model AI popełni błąd (np. skutek halucynacji lub ataku), sam token uniemożliwi wykonanie nieautoryzowanej transakcji. Mastercard współpracuje z organizacją FIDO Alliance nad globalnym standardem weryfikacji płatności. Rozwiązanie to wymaga biometrycznego potwierdzenia operacji przez konsumenta. Dzięki temu każde polecenie wykonane przez algorytm posiada niepodważalny dowód świadomej zgody człowieka.

Podejście agnostyczne – Stripe ACP oraz Google AP2

Z perspektywy firm wspierających wdrożenia e-commerce wiodącym standardem stał się Agent Commerce Protocol (ACP) opublikowany przez Stripe w bliskiej współpracy z OpenAI.

Sklep internetowy musi udostępnić dedykowane interfejsy (API RESTful lub MCP), aby mógł współpracować z zewnętrznym algorytmem AI, zgodnie z zasadami ACP. Pozwala to systemowi wysyłać polecenia tworzenia i aktualizacji koszyka.

Model bezpieczeństwa Stripe opiera się na generowaniu specjalnego tokena, który AI przydziela sprzedawcy w imieniu klienta, ustalając jednocześnie limit kwoty oraz czas wygaśnięcia. Prywatny moduł rozliczeniowy przetwarza ten token w taki sposób, że sam model LLM nie widzi wrażliwych danych, co skutecznie zapobiega nadużyciom i próbom przejęcia uprawnień. Stripe uzupełnił ten protokół wytycznymi technicznymi, które nakazują sklepom udostępnianie plików konfiguracyjnych działających jak czytelne dla algorytmów słowniki określające dopuszczalne reguły nawigacji.

Inicjatywa Google, Agent Payments Protocol (AP2), opiera się o odmienną filozofię: zaawansowaną konstrukcję kryptograficznie zabezpieczonych autoryzacji, stanowiących de facto serię mikrokontraktów. Pierwszym krokiem jest autoryzacja upoważniająca proces AI do wyszukania opcji w ustalonym budżecie. Gdy rozwiązanie wybierze konkretne produkty, oddzielny zapis zatwierdza koszyk. Dopiero wtedy odpowiedni sygnał uruchamia sieć autoryzacyjną i zamyka całą sekwencję.

Ekosystem Agent Commerce budują także firmy spoza tradycyjnych sieci kartowych. Klarna, europejski lider płatności odroczonych, uruchomiła asystenta AI opartego na technologii OpenAI. W pierwszym miesiącu algorytm obsłużył 2,3 miliona rozmów, co stanowiło dwie trzecie wszystkich czatów w dziale wsparcia. Narzędzie to wykonało pracę równą 700 pełnoetatowym konsultantom i skróciło czas rozwiązania problemu z 11 do niecałych 2 minut. W trzecim kwartale 2025 roku asystent AI Klarny wykonywał pracę 853 agentów, generując oszczędności rzędu 60 milionów dolarów rocznie.

Z kolei FIS, jeden z największych globalnych dostawców infrastruktury finansowej, w styczniu 2026 roku uruchomił pierwszą w branży platformę agentic commerce umożliwiającą bankom bezpieczne przetwarzanie transakcji inicjowanych przez agentów AI. Platforma opiera się na frameworku Know Your Agent (KYA) do identyfikacji systemów AI i współpracuje z Visa Intelligent Commerce oraz Mastercard. Według FIS adopcja AI wśród banków wzrosła ośmiokrotnie w porównaniu z 2023 rokiem.

5.2

Visa i Mastercard – wspólny cel, różne metody budowania zaufania

Visa i Mastercard nie są bankami, ale to one pracują nad rozwiązaniem najtrudniejszego problemu w Agentic Banking. Wyzwanie polega na tym, aby algorytm mógł działać w imieniu klienta bez łamania procedur autoryzacji, odpowiedzialności czy kontroli oszustw. Rozwiązanie musi być przejrzyste dla wydawców kart i wygodne dla sprzedawców.

Deloitte wskazuje firmy Visa, Mastercard i PayPal jako graczy eksperymentujących z nowoczesnym handlem. Najbliższa fala autonomii AI w finansach będzie opierać się na systemach rozliczeniowych i poświadczeniach wspartych protokołami komunikacyjnymi. Same modele językowe schodzą tutaj na dalszy plan.



Autoryzacja brzegowa
(Cloudflare/Edge),
protokół TAP.

Tokenizacja (brak prawdziwych
numerów kart w AI), twarde limity
transakcji, pełna i natychmiastowa
odwoływalność zgód przez klienta.



Standard FIDO
(Verifiable Intent),
koncepcja zaufanych
"Agentic Tokens".

Visa – od tokenizacji kart do innowacyjnej ekonomii

Środowisko testowe Visa Intelligent Commerce ruszyło w kwietniu 2025 roku przy współpracy z firmami Anthropic, IBM, Microsoft, Mistral AI, OpenAI, Perplexity, Stripe i Samsung. Szerokie wdrożenia rynkowe zaplanowano na obecny, 2026 rok. Lista partnerów pokazuje skalę projektu. Dzięki temu rozwiązaniu narzędzia Agentic Banking z różnych ekosystemów mogą bezpośrednio realizować transakcje przez infrastrukturę firmy Visa.

Zamiast przekazywać surowe dane karty, użytkownicy korzystają z cyfrowych poświadczeń przygotowanych pod obsługę przez AI. System działa w imieniu klienta dopiero po jego wyraźnej aktywacji. Konsument zachowuje pełną kontrolę, ustalając limity wydatków oraz warunki każdej operacji. Dzięki przesyłaniu sygnałów handlowych bezpośrednio do sieci Visa, instytucja może skutecznie blokować oszustwa i rozstrzygać spory. Cały mechanizm opiera się na delegowaniu uprawnień – każda zgoda posiada przypisaną politykę kosztów, którą właściciel konta może w każdej chwili wycofać.

Dokumentacja techniczna wskazuje, że procesy AI wymagają sztywnych budżetów i tokenizacji, ponieważ rynek wciąż ustala zasady odpowiedzialności za błędy czy nadużycia. Visa wymaga możliwości natychmiastowego odwołania dostępu lub jego zmiany, gdy zmieniają się warunki transakcji. Nadzór człowieka jest niezbędny, szczególnie przy dużych kwotach lub operacjach objętych restrykcjami prawnymi. Nawet najwięksi dostawcy infrastruktury uznają, że pełna autonomia bez ręcznego hamulca bezpieczeństwa nie jest rozwiązaniem docelowym.

W październiku 2025 roku Visa i Cloudflare wprowadziły Trusted Agent Protocol. To rozwiązanie pozwala sklepom odróżnić zweryfikowane systemy AI od szkodliwych botów. W programie testowym uczestniczą już tacy giganci jak Stripe, Shopify czy Adyen. Ta zmiana jest kluczowa dla wydawców kart, ponieważ automatyczne płatności wymagają jednoczesnego potwierdzenia dwóch rzeczy: zgody klienta oraz wiarygodnej tożsamości samego oprogramowania, które składa zamówienie.

We wrześniu 2025 roku Visa udostępniła MCP Server oraz Acceptance Agent Toolkit. Ten zestaw narzędzi pozwala modelom AI bezpiecznie łączyć się z systemem Visa Intelligent Commerce. Rozwiązanie to obsługuje również tryby niewymagające kodowania, co umożliwia fakturowanie czy generowanie linków płatniczych za pomocą zwykłych poleceń tekstowych. Visa tworzy w ten sposób kompletną platformę operacyjną dla Agentic Banking, wychodząc poza prosty produkt płatniczy. W pilotażowych wdrożeniach, prowadzonych między innymi z firmą Aldar w Zjednoczonych Emiratach Arabskich, modele AI samodzielnie opłacają już stałe rachunki, takie jak opłaty serwisowe.

Mastercard. Agent Pay i architektura potwierdzania

Zasady Mastercard Agent Pay Acceptance Framework wymagają, aby każda instancja AI została zarejestrowana i zweryfikowana przed wykonaniem płatności. Systemy muszą być jednoznacznie identyfikowalne, a same operacje wykorzystują dynamiczne poświadczenia, które gwarantują śledzenie każdej transakcji. Sprzedawcy mogą rozpoznawać autoryzowane procesy już na etapie przesyłu danych dzięki standardowi Web Bot Auth. Zamiast wymuszać przebudowę całego

internetu, Mastercard wbudowuje mechanizmy weryfikacji w istniejące formularze płatnicze przy pomocy specjalnych kodów.

Firma buduje jasny model weryfikacji oprogramowania, ponieważ samo posiadanie danych karty to za mało. Sieć sprawdza teraz, który konkretnie system wykonuje płatność, na jakiej podstawie i z jakim limitem wydatków. Taki kierunek zmienia tradycyjną autoryzację typu „tak lub nie” w złożoną ocenę kontekstu, w jakim klient przekazał uprawnienia maszynie.

Mastercard łączy te rozwiązania z biometrią i kluczami dostępu w ramach Payment Passkey Service. Współpraca z partnerami takimi jak Microsoft, IBM, Braintree czy Checkout.com pozwala wdrażać te funkcje zarówno w handlu detalicznym, jak i w relacjach B2B. Płatności uruchamiane przez automatyczne systemy to dla Mastercard kolejny etap odchodzenia od ręcznego wpisywania danych na rzecz programowalnych poświadczeń.

Co łączy Visa i Mastercard

Visa i Mastercard dążą do tego samego: wprowadzenia uprawnień warunkowych. Różnią się metodą – Visa stawia na weryfikację w węzłach sieci i protokół TAP, natomiast Mastercard wybiera tokeny z zaszytymi regułami oraz standard FIDO. Obie firmy łączy jednak twarda zasada: system AI dostaje tylko tyle uprawnień, ile wyznaczy klient lub bank, a każdą zgodę można natychmiast cofnąć. Dowolność w dysponowaniu pieniędzmi jest wykluczona.

Z tej strategii wynikają trzy wnioski. Agentic Banking rozwinie się szybciej w handlu internetowym i na kartach niż w zwykłych przelewach, ponieważ tamtejsza infrastruktura jest już na to gotowa. Banki mogą umocnić swoją pozycję, jeśli wdrożą nowe systemy weryfikacji i zaczną rygorystycznie pilnować polityk dostępu. O sukcesie rozstrzygnie skuteczna kontrola nad tym, komu i na co klient pozwolił, a same modele językowe będą tu tylko dodatkiem

Szerszy ekosystem. PayPal, Stripe i protokoły dla handlu

Visa i Mastercard działają w otoczeniu wielu konkurencyjnych rozwiązań. Stripe rozwija ograniczone tokeny płatnicze oraz protokół ACP, a PayPal buduje usługi handlowe na własnej infrastrukturze, łącząc weryfikację tożsamości z ochroną kupującego. Firma ta współpracuje z Mastercardem oraz twórcami narzędzi AI. Z europejskiej perspektywy istotny jest również ruch Revolut Pay w stronę standardu AP2. Płatności w modelu Agentic Banking będą prawdopodobnie korzystać z wielu protokołów jednocześnie. Model zamknięty, oparty na technologii tylko jednego dostawcy, jest mało prawdopodobny.

Najważniejsze wnioski



Rynek tworzy nowe standardy płatności dla maszyn: Visa TAP, Mastercard Agent Pay, Stripe ACP i Google AP2.



Podstawą bezpieczeństwa jest tokenizacja, która ukrywa wrażliwe dane kart przed sztuczną inteligencją.



Nowe rozwiązania pozwalają maszynie wykonać płatność tylko w określonym czasie i ustalonych z góry limitach.



Agentic Banking łatwiej podpiąć pod infrastrukturę do obsługi kart niż pod tradycyjne przelewy bankowe.



Nowe zagrożenia

– jak przestępcy wykorzystują AI przeciwko bankom?

6.1

Adversarial AI – ewolucja zagrożeń dla infrastruktury cyfrowej

Metody hakerskie zmieniają się wraz z całą gospodarką, przez co w 2026 roku sztywne skrypty masowej automatyzacji tracą znaczenie na rzecz autonomicznych i zdecentralizowanych systemów atakujących. Tradycyjne zabezpieczenia oparte na sztywnych regułach przestają działać, ponieważ działania przestępców coraz skuteczniej naśladują ruch autoryzowanych użytkowników oraz wewnętrznych narzędzi bankowych.

Nowe kategorie oszustw wykorzystujących AI obejmują między innymi:

Polimorficzny phishing (Polymorphic Phishing) polegający na przejęciu firmowej domeny pocztowej, gdzie zamiast wysyłania prymitywnych wiadomości z podejrzanymi linkami, system miesiącami analizuje historię korespondencji. Pozwala to algorytmowi poznać styl wypowiedzi oraz wewnętrzny żargon ofiary, aby w kluczowym momencie, np. podczas zatwierdzania płatności, wygenerować sfałszowaną wiadomość z podmienionym numerem rachunku. Zabezpieczenia reagujące jedynie na zainfekowane strony przepuszczają taki komunikat, uznając go za naturalną część autentycznego wątku biznesowego.

Oprogramowanie szpiegowskie używane w Predictive Payment Impersonation analizuje kalendarz przelewów ofiary, aby uderzyć dokładnie w terminie rozliczeń. Złośliwy algorytm przesyła sugestijną informację o zmianie warunków faktury tuż przed nadejściem prawdziwego dokumentu od stałego dostawcy. Wywołany w ten sposób chaos w działach księgowych sprawia, że sfałszowane dane przechodzą przez kontrolę bez należytej czujności.

Metody Hardware-Assisted KYC Bypass oraz usługi Deepfake as a Service skutecznie podważają wiarygodność zdalnego onboardingu i identyfikacji biometrycznej. Atakujący wykorzystują specjalnie przygotowane systemy wirtualne, które oszukują aplikacje finansowe poprzez podłożenie spreparowanego obrazu wysokiej rozdzielczości bezpośrednio pod systemowy sterownik aparatu w telefonie.

Autonomiczne modele AI tworzące Synthetic Identity Farms miesiącami budują wiarygodną historię fikcyjnych rachunków. Algorytmy terminowo spłacają drobne raty i zarządzają lokatami, aby uzyskać wysokie oceny kredytowe. Po zdobyciu zaufania systemu sztuczne tożsamości

przeprowadzają skoordynowaną akcję, zaciągając jednocześnie kredyty na dziesiątki milionów euro i wyprowadzając środki przez rozproszone przelewy zagraniczne.

Wstrzykiwanie złośliwych poleceń (Prompt Injection) uderza bezpośrednio w warstwę konwersacyjną bankowych asystentów. Podatne na ataki boty, pozbawione odpowiednich filtrów, wykonują instrukcje ukryte w zapytaniach użytkowników. Takie działania zmuszają systemy do omijania blokad finansowych lub ujawniania danych wrażliwych, co obciąża bank pełną odpowiedzialnością prawną i wizerunkową.

Organizacje finansowe na przełomie 2025 i 2026 roku zastępowaty jednoetapową weryfikację tożsamości ciągłym nadzorem operacji w czasie rzeczywistym. Nowy standard bezpieczeństwa wymaga autoryzacji samego narzędzia płatniczego zintegrowanego z systemem bankowym, co określa się terminem Know Your Agent.

Nowe wektory cyberataków (Adversarial AI)



Polimorficzny Phishing

AI generuje maile, idealnie kopiując styl pisanego, żargon i historię korespondencji ofiary (zero błędów, perfekcyjny kontekst).



Predictive Impersonation

Atak w punkt. AI uderza w konkretnym oknie rozrachunkowym, podając się za zaufanego dostawcę, gdy księgowość spodziewa się faktury.



Deepfake KYC Bypass

Wstrzykiwanie wygenerowanego przez AI wideo bezpośrednio do wirtualnych kamer smartfona (obejście sprawdzania "liveness").



Farmy Syntetyczne

Boty masowo budujące idealną historię kredytową dla wymyślonych tożsamości, by po roku dokonać jednorazowego, gigantycznego wyłudzenia.

6.2

Raportowanie ESG i zrównoważony rozwój (CSRD) w obliczu wdrażania AI

Zielone rozwiązania AI w chmurze często mają duży koszt środowiskowy, co sprawia, że są poważnym wyzwaniem dla audytorów bankowych w kontekście rosnących wymagań UE dotyczących śladu węglowego. Nowa unijna dyrektywa o sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (CSRD) poszerza krąg instytucji oraz narzuca surowe i obligatoryjne standardy ujawniania (ESRS) korelacji finansowania i działań biznesowych ze wskaźnikami klimatycznymi na szeroką skalę już od 2024 roku, a od 2026 staje się to konieczne także dla podmiotów niefinansowych w Europie powiązanych z sektorem.

Dostawcy usług chmurowych generują ogromne zapotrzebowanie na energię, które do 2030 roku ma wzrosnąć z 25 GW do aż 120 GW. Tak duża skala operacji narzuca wysoki ślad węglowy i materiałowy na serwery, które banki wynajmują do obsługi platform AI. Obciąża to bezpośrednio kalkulacje emisji w łańcuchu wartości (Scope 3), obejmującym złożoną sieć powiązań poza fizyczną kontrolą instytucji finansowej. W świetle przepisów CSRD banki muszą raportować i dokładnie szacować te wszystkie pośrednie koszty logistyczne.

Tymczasem te same banki, zmuszone do raportowania wskaźników finansowanych aktywów (GAR), coraz częściej wyręczają się w tym zadaniu algorytmami. Systemy wykorzystujące technologię RAG błyskawicznie sprawdzają listy klientów biznesowych, analizując tysiące stron sprawozdań finansowych i audytów bez angażowania pracowników. Taka automatyzacja pochłania jednak ogromną moc obliczeniową, co generuje wysokie zużycie energii. Przez te ukryte koszty energetyczne banki muszą dokładniej wyliczać swój realny wpływ na środowisko, aby spełnić unijne normy i przejść kontrole EBC.

Najważniejsze wnioski



Tradycyjne zabezpieczenia są czasami bezradne w starciu z atakami wykonywanymi przez AI.



Cyberprzestępcy atakują precyzyjnie – uderzają w konkretnych dniach rozliczeniowych i idealnie podrabiają styl maili ofiary.



Oszuści masowo używają deepfake'ów, żeby ominąć kamery podczas weryfikacji tożsamości.



AI zużywa w chmurze potężne ilości energii, co psuje bankom statystyki i utrudnia raportowanie ESG.

Najlepsze przykłady z rynku

W 2026 roku najlepsze wyniki przynoszą wdrożenia, które łączą dużą skalę z konkretnym zyskiem, dają się ująć w jasne ramy i nie podlegają najsurowszym rygorom prawnym. Najlepiej sprawdzają się rozwiązania w obsłudze klienta, zwalczaniu oszustw, procesach wewnętrznych oraz kontroli AML. Pełna autonomia w kredytach czy zarządzaniu majątkiem wciąż przegrywa z nadmiarem procedur.

Wykrywanie oszustw i reklamacje

To obecnie najsukuteczniejsze zastosowanie systemów Agentic Banking. Banki mają tu jasne wskaźniki efektywności, a algorytmy potrafią samodzielnie zebrać dane, zablokować podejrzone operacje i przygotować sprawę dla pracownika. Taką ścieżkę rozwoju buduje m.in. [NatWest](#).

Codzienna obsługa w aplikacji

Wyjaśnianie opłat, analiza historii, zarządzanie subskrypcjami czy zmiana limitów kart to zadania, w których AI radzi sobie bez pomocy personelu. Systemy takie jak Erica ([Bank of America](#)) czy Cora ([NatWest](#)) udowadniają, że większość rutynowych zapytań można zamknąć bez udziału człowieka.

Zarządzanie budżetem i coaching finansowy

To priorytet dla bankowości detalicznej ze względu na dużą wartość dla klienta i niskie koszty wdrożenia. O ile system nie udaje certyfikowanego doradcy, pozostaje bezpieczny pod względem prawnym. Rozwiązania te rozwijają m.in. [Lloyds](#), [N26](#), [Revolut](#) i [Bank of America](#).

Wsparcie pracowników i administracji

Automatyzacja pracy biurowej przynosi najszybszy zwrot z inwestycji. Algorytmy streszczają rozmowy, wyszukują procedury i przygotowują odpowiedzi, co drastycznie obniża koszty obsługi. Według [McKinsey](#) odpowiednie przeprojektowanie tych procesów pozwala na skokowy wzrost produktywności.

Weryfikacja KYC i alerty AML

Modele AI idealnie nadają się do wieloetapowej analizy dokumentów i wykrywania nietypowych przelewów. [ING](#) wykorzystuje te technologie do tropienia podejrzanych wzorców, a nadzór EBA wskazuje walkę z praniem pieniędzy jako jeden z najbardziej zaawansowanych obszarów zastosowań.

Koordinacja procesów kredytowych

AI nie podejmuje jeszcze samodzielnych decyzji o przyznaniu kredytu, ale przejmuje całą biurokrację. Systemy zbierają dokumenty, wypełniają formularze i przygotowują pakiety danych do oceny kredytowej. [McKinsey](#) szacuje, że takie wsparcie podnosi wydajność pracy od 40 do nawet 80%.

Wirtualni asystenci dla firm i sektora MŚP

Doświadczenia systemu [DBS Joy](#) potwierdzają, że w bankowości korporacyjnej maszyny mogą prowadzić większość bieżących relacji z klientem. W tym modelu system rozwiązuje rutynowe problemy, a przy skomplikowanych sprawach przekazuje klienta do specjalisty, który korzysta z podpowiedzi programu. W Europie takie rozwiązanie obniża wysokie koszty obsługi małych firm, zapewniając im jednocześnie szybkie odpowiedzi.

Automatyczne płatności o niskim ryzyku

Nowoczesne metody autoryzacji zakupów nie są jeszcze w UE zjawiskiem masowym, ale stanowią kluczowy kierunek strategiczny. W 2026 roku najbardziej realne scenariusze obejmują płatności u zaufanych sprzedawców, określone kategorie zakupów z limitami kwotowymi oraz opłacanie domowych rachunków. Właśnie w tę stronę rozwijają się systemy [Visa](#), [Mastercard](#), [Stripe](#), [PayPal](#) oraz [Revolut](#).

Zysk \ Gotowość	Gotowość		
	Mała	Średnia	Duża
Mały			
Średni			Szybkie wdrożenie Podsumowanie wydatków, delegowanie stałych opłat domowych, koordynacja wniosków kredytowych (zbieranie danych).
Wysoki	Blokady regulacyjne – Opuścić W pełni autonomiczne decyzje o przyznaniu kredytu, autonomiczne zarządzanie majątkiem i inwestycjami.		Robić to Wykrywanie fraudów, asystent call center, codzienna obsługa w aplikacji, wstępna analiza KYC/AML.

Najważniejsze wnioski



Agentic Banking sprawdza się dziś najlepiej przy wykrywaniu oszustw i masowej obsłudze zapytań klientów.



Zamiast doradzać (co jest ryzykowne prawnie), AI powinna skupić się na analizie wydatków i nawigowaniu klienta.



Sztuczna inteligencja jako asystent pracownika call center tnie koszty i nie naraża banku na to, że maszyna sama podejmie złą decyzję.



AI może zebrać dokumenty i przygotować proces kredytowy, ale ostateczną decyzję zawsze musi podjąć człowiek.

Plan działania

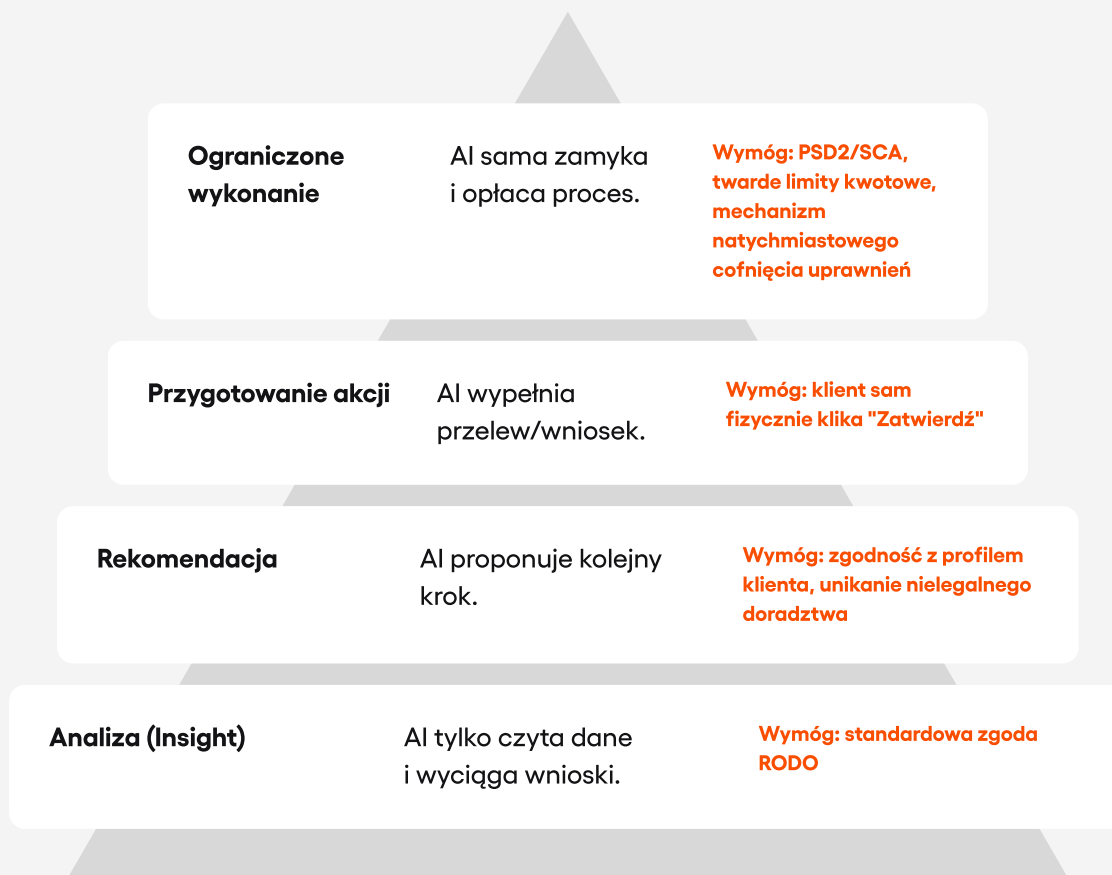
– co wdrożyć teraz, a co może poczekać?

Zamiast budować jednego asystenta do wszystkiego, banki powinny rozdzielić uprawnienia na cztery etapy: analizę danych, tworzenie rekomendacji, przygotowanie operacji oraz jej wykonanie w ramach limitów. Taki podział ułatwia wskazanie odpowiedzialnych za błędy i przeprowadzenie audytu, co jest kluczowe przy przepisach AI Act oraz standardach Visa i Mastercard.

Przy projektowaniu produktów najlepiej skupić się na zadaniach o dużej skali, ale niskim ryzyku prawnym. Wykrywanie oszustw, codzienna obsługa, analiza wydatków czy weryfikacja klientów (KYC/AML) to obszary, w których najłatwiej zmierzyć zyski i wyznaczyć algorytmom sztywne granice.

W płatnościach banki muszą stworzyć własny system zarządzania zgodami, oparty na tokenizacji, nowoczesnych kluczach dostępu i limitach. Ważne, aby te rozwiązania od początku trafiły do głównych systemów banku. Izolowanie ich jako pobocznych „projektów innowacyjnych” sprawia, że szybko przestają one odpowiadać realnym wymogom rynkowym.

Możliwość natychmiastowego przerwania automatycznego procesu i przejęcia sprawy przez pracownika musi być dostępna od samego początku. Dodawanie takich bezpieczników dopiero po awarii drastycznie podnosi koszty i ryzyko wdrożenia.



Niezbędne jest też wyraźne oddzielenie edukacji finansowej od doradztwa inwestycyjnego oraz zbierania danych od podejmowania ostatecznych decyzji kredytowych. Same dopiski w regulaminach nie wystarczą – produkt musi być tak skonstruowany, by jego rozwój nie zagrażał stabilności biznesu.

Na poziomie strategii awarie chmury czy błędy modeli powinny być tematem dla zarządu i komitetów ryzyka, a nie tylko dla informatyków. Ponieważ innowacje zależą od zewnętrznych dostawców, banki muszą mieć gotowe plany awaryjne i rygorystycznie pilnować jakości na każdym etapie współpracy.

Najważniejsze wnioski



Banki powinny wdrażać AI stopniowo – od zwykłej analizy po ściśle limitowane płatności.



Zespoły produktowe powinny skupić się na prostych, masowych operacjach, gdzie ewentualna pomyłka maszyny niewiele kosztuje.



Banki muszą od razu projektować system tak, aby żywy doradca mógł w każdej chwili przerwać działanie maszyny i cofnąć jej decyzję.



Uzależnienie od dostawców chmury i AI to już problem bezpośrednio dla zarządów, a nie tylko dla działu IT.

Konkluzja

Sukces technologii Agentie Banking zależy od zaufania ludzi, dlatego samo jej uruchomienie nie gwarantuje masowego użycia. Bez akceptacji klientów nawet najbardziej autonomiczne rozwiązania nie zyskają popularności. W 2026 roku największe szanse mają te wdrożenia, które przejmują konkretne zadania w jasno określonych granicach. Pełne zastąpienie bankiera pozostaje wizją odległą i prawnie niemożliwą, więc banki skupiają się na wykrywaniu oszustw, obsłudze klienta, weryfikacji KYC/AML oraz pilnowaniu etapów spraw. Kierunki wyznaczone przez Visa i Mastercard potwierdzają, że przyszłość automatyzacji w finansach opiera się na precyzyjnych uprawnieniach, które klient lub bank mogą w dowolnej chwili cofnąć.

Przewagę zyskają instytucje, które najlepiej dopracują sposób przekazywania zadań algorytmom. To właśnie ta metoda zdecyduje o tym, jak szybko i bezpiecznie bank rozszerzy zakres obowiązków AI wraz z rosnącym zaufaniem ze strony regulatorów i klientów. W ciągu najbliższych dwóch lub trzech lat najważniejszym sprawdzianem dojrzałości będzie umiejętność sprawnego zarządzania tymi uprawnieniami przy zachowaniu pełnej jasności każdej decyzji.