

# Nadużycia w sektorze finansowym

edycja

**2025**

**Z | P | F**

Związek  
Przedsiębiorstw  
Finansowych  
w Polsce



Shape the future  
with confidence

Raport został opracowany przez zespół w składzie:  
Katarzyna Łukasik-Gogol  
Laura Benachir  
Zuzanna Łubińska

Wsparcia merytorycznego w formie wywiadów eksperckich udzieliłi:  
Katarzyna Baumgart  
Maciej Mittag  
Piotr Raubo  
Bartosz Wójcicki

Gdańsk/Warszawa, październik 2025

COPYRIGHT

© Związek Przedsiębiorstw Finansowych w Polsce  
© Ernst & Young spółka z ograniczoną odpowiedzialnością Consulting spółka komandytowa

Związek Przedsiębiorstw Finansowych w Polsce  
ul. Długie Pobrzeże 30  
80-888 Gdańsk  
[www.zpf.pl](http://www.zpf.pl)

Ernst & Young spółka z ograniczoną odpowiedzialnością Consulting spółka komandytowa  
Rondo ONZ 1  
00-124 Warszawa  
[www.ey.com/pl](http://www.ey.com/pl)

# Spis treści

Słowo wstępne	4
Wprowadzenie	8
Uczestnicy badania	10
Szczegółowe wyniki badania	12
Obraz ryzyka nadużyć w sektorze finansowym	13
Narzędzia przeciwdziałania nadużyciom	21
Nadużycia przyszłości, przyszłość nadużyć	27
Współpraca z organami ścigania	29
Podsumowanie	32





Sektor finansowy funkcjonuje dziś w otoczeniu nieustannie rosnących wymogów regulacyjnych, które stanowią zarówno tarczę bezpieczeństwa, jak i wyzwanie operacyjne dla instytucji. Dynamiczny rozwój technologii oraz lawinowy wzrost transakcji online niosą nie tylko nowe możliwości, lecz także generują coraz bardziej złożone zagrożenia. Schematy nadużyć ulegają ciągłym zmianom – sprawcy błyskawicznie adaptują się do nowych rozwiązań i luk systemowych, co wymaga od nas nieustannej czujności oraz elastycznego podejścia do strategii przeciwdziałania.

Raport przygotowany wspólnie przez Związek Przedsiębiorstw Finansowych oraz EY Polska koncentruje się nie tylko na analizie skali oszustw, ale również na tym, jak sektor dostosowuje narzędzia do zmieniających się metod działania sprawców. W tym kontekście kluczowe staje się wdrażanie innowacyjnych mechanizmów detekcji oraz rozwijanie kompetencji zespołów, które muszą działać sprawnie w dynamicznie zmieniającym się środowisku branżowym.

Dziękuję wszystkim uczestnikom badania za ich wkład i otwartość w dzieleniu się doświadczeniami. Mam nadzieję, że niniejszy raport wniesie wartość nie tylko w obszarze analizy zagrożeń, lecz przede wszystkim w rozwoju nowoczesnych strategii i praktyk, pozwalających skuteczniej chronić rynek finansowy przed stale zmieniającymi się formami nadużyć.

**Mariusz Witalis**  
Partner,  
EY Polska



W 2024 roku w Polsce zostało zidentyfikowanych prawie 46 tys. domen internetowych powiązanych z procederem namawiania użytkowników na fałszywe inwestycje. Ta liczba jest porażająca, zwłaszcza gdy uświadomimy sobie, że paleta sztuczek socjotechnicznych jest znacznie większa. W przestępczym świecie rośnie rola usług phishing-as-a-service (PhaaS) – nawet osoby bez wiedzy technicznej mogą przekwalifikować się w oszustów i zarabiać na zamówionych wcześniej fałszywych stronach sklepów internetowych czy banków.

Z drugiej strony mamy instytucje finansowe, których obowiązkiem jest ochrona konsumentów. Większość podmiotów przyznaje, że to zbyt rozbudowane przepisy hamują skuteczniejszą walkę z nadużyciami. Sami zaś klienci często domagają się rekompensat po utracie środków, nawet gdy dali się zmanipulować. Trudno nie odnieść wrażenia, że w wielu takich sytuacjach czują się zwolnieni z odpowiedzialności za własne decyzje.

Raport z tegorocznego badania nadużyć w sektorze finansowym pokazuje, że rynek powinien nieustannie szukać nowych, powiązanych ze sobą rozwiązań na poziomie technologii, regulacji i edukacji, by lepiej bronić się przed oszustami.

Dziękuję EY Polska oraz uczestnikom badania za chęć podzielenia się wiedzą i doświadczeniem. Jestem przekonany, że ten raport pozwoli lepiej zrozumieć zmieniające się trendy w obszarze fraudów.

Zapraszam do lektury!

**Marcin Czugań**  
Prezes Zarządu,  
Związek Przedsiębiorstw  
Finansowych w Polsce



Przeciwdziałanie fraudom od wielu lat jest kluczowym obszarem działalności Związku Polskiego Leasingu. Z samej idei leasingu, w której firma leasingowa bierze na siebie ryzyko nie tylko udzielonego finansowania, lecz także jego przedmiotu, wynika, że część ryzyk jest taka sama jak przy finansowaniu kredytem, a część specyficzna jedynie dla naszego segmentu rynku. Jak pokazują tegoroczne i wcześniejsze badania, należą do nich przede wszystkim przywłaszczenia i kradzież przedmiotu leasingu. Jednocześnie uczestnicy badania podkreślają, że największe problemy w skutecznym przeciwdziałaniu fraudom mają właśnie z tymi zdarzeniami. Dlatego tak istotna w tym obszarze jest szybkość i skuteczność działania organów ścigania.

Niezależnie od ryzyk związanych z przedmiotem leasingu, firmy leasingowe dużą wagę przy podejmowaniu decyzji o przyznaniu finansowania przywiązują do weryfikacji danych klientów. Tutaj również mamy sporo wyzwań, szczególnie z uwagi na ograniczone możliwości weryfikacji przedstawianych dokumentów. Dotyczy to zarówno dokumentów finansowych klienta (brak dostępu do rejestrów skarbowych), jak i wiarygodności dokumentacji przedmiotu leasingu (dokumentów zakupu, udokumentowanej historii szkód itp.).

Każdy kwartał przynosi poprawę w zakresie walki z nadużyciami, dlatego w kolejnej edycji badania mamy nadzieję na lepsze wyniki w obszarze zabezpieczeń przed wyłudzeniami w firmach leasingowych.

Dziękując podmiotom uczestniczącym w badaniu, zapraszam wszystkich do zapoznania się z jego wynikami.

**Monika Constant**  
Prezeska Zarządu,  
Związek Polskiego  
Leasingu



Mamy przyjemność oddać w Państwa ręce 18 edycję raportu *Nadużycia w sektorze finansowym*, opracowanego wspólnie przez EY Polska oraz Związek Przedsiębiorstw Finansowych (ZPF). Publikacja ta powstała w ramach wieloletniego projektu badawczego ukierunkowanego na monitorowanie skali i charakteru zjawiska nadużyć w branży finansowej w Polsce.

W niniejszym raporcie przedstawiamy kluczowe wyzwania, przed którymi stoi rynek finansowy w zakresie przeciwdziałania nadużyciom. Podobnie jak w poprzednich latach, zapytaliśmy instytucje finansowe, jakie działania podejmują w odpowiedzi na narastającą skalę oszustw. Zwróciliśmy także uwagę na nowe zagrożenia, w tym te związane z cyberprzestępczością, socjotechniką oraz wykorzystaniem nowoczesnych technologii.

Raport ten, poza analizą statystyczną i oceną instytucjonalnych mechanizmów przeciwdziałania nadużyciom, uwzględnia również kluczowe wyzwania dotyczące stosowania nowoczesnych metod detekcji czy też dużej liczby regulacji, w kontekście zwiększającego się poziomu zaawansowania schematów nadużyć, coraz częściej wykorzystywanych przez sprawców.

Badanie zostało przeprowadzone w formie anonimowej ankiety wśród przedstawicieli sektora finansowego w okresie od marca do czerwca 2025, a zakres analizy objął cały 2024 rok. Warto dodać, że w tegorocznym badaniu część okresu badawczego (tj. okres od stycznia do maja 2024) pokrywa się z tym z poprzedniej edycji, w której to analizowano ostatnie 12 miesięcy do momentu wypełniania formularza.

Podobnie jak w zeszłym roku, w uzupełnieniu do badania ankietowego przeprowadzono wywiady eksperckie z przedstawicielami instytucji finansowych. Celem rozmów było zebranie dodatkowych informacji na temat sposobów przeciwdziałania nadużyciom w sektorze finansowym. Tegoroczne badanie zostało także uzupełnione o dane z międzynarodowych raportów, obejmujące m.in. trendy w wykorzystywaniu nowych technologii, zagrożenia cybernetyczne oraz najczęstsze kanały popełniania oszustw finansowych. Zebrane informacje wskazują na transgraniczny charakter nadużyć i możliwe kierunki działań prewencyjnych.

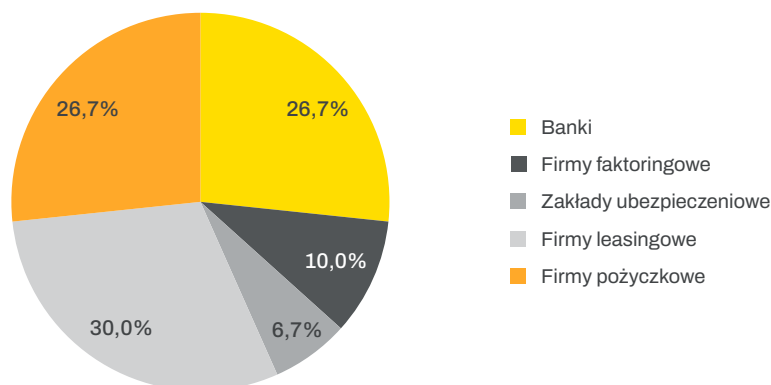
Jako zespół EY Polska i ZPF dziękujemy wszystkim osobom i instytucjom, które przyczyniły się do powstania raportu, za udostępnione dane i merytoryczne zaangażowanie. Celem publikacji jest przedstawienie aktualnych informacji wspierających uczestników rynku finansowego w rozwijaniu strategii przeciwdziałania nadużyciom. Zaprezentowane analizy mogą stanowić użyteczne narzędzie przy podejmowaniu decyzji związanych z ograniczaniem ryzyka oszustw i wzmocnieniem bezpieczeństwa operacyjnego.



Wśród ankietowanych tegorocznej edycji badania znalazły się firmy leasingowe (30%), banki i instytucje pożyczkowe, które stanowiły po 26,7% respondentów, a także firmy faktoringowe (10%) i zakłady ubezpieczeń (6,7%). Udział poszczególnych sektorów w tegorocznym badaniu ilustruje wykres 1.

**Wykres 1.** Rodzaje instytucji biorących udział w badaniu

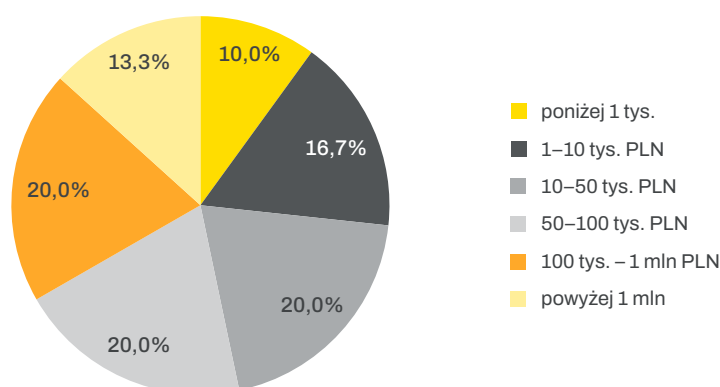
Źródło: ZPF/EY.



Biorąc pod uwagę wielkość instytucji, mierzoną liczbą aktywnych klientów na koniec 2024 roku, w tegorocznym badaniu uczestniczyły podmioty o zróżnicowanej skali operacyjnej, przy czym żadna z grup nie jest wyraźnie dominująca. Organizacje obsługujące poniżej tysiąca klientów stanowiły 10% ogólnej liczby podmiotów biorących udział w badaniu i wśród nich dominowały firmy faktoringowe. Przedział od 1 do 10 tys. klientów zadeklarowało 16,6% instytucji. Najliczniejsze grupy respondentów (po 20% każda) stanowiły podmioty obsługujące odpowiednio: od 10 do 50 tys., od 50 do 100 tys. oraz od 100 tys. do 1 mln osób. Obsługę powyżej 1 mln aktywnych klientów deklarowało 13,3% respondentów w tym głównie banków oraz zakłady ubezpieczeń.

**Wykres 2.** Liczba aktywnych klientów w badanych instytucjach na koniec 2024 roku

Źródło: ZPF/EY.



Badanie instytucji o różnej wielkości umożliwiło równoległą analizę wyzwań, z jakimi mierzą się zarówno największe, jak i mniejsze podmioty rynku finansowego. Takie zróżnicowanie próby umożliwia porównanie podejść i identyfikację specyficznych potrzeb oraz rozwiązań, które sprawdzają się w różnych segmentach rynku. Otrzymane wyniki pozwalają na formułowanie wniosków dostosowanych do praktyki zarówno dużych, jak i mniejszych organizacji.



## Obraz ryzyka nadużyć w sektorze finansowym

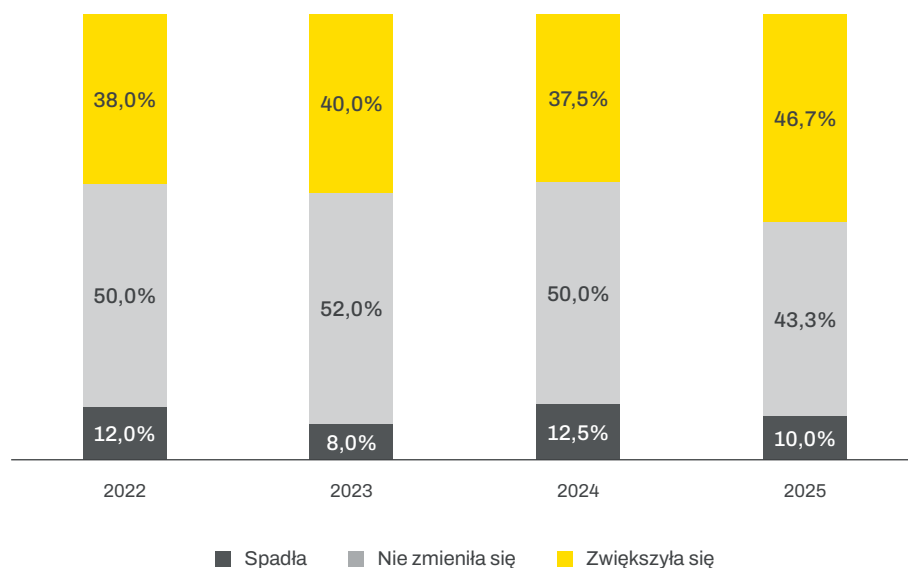
Zjawisko nadużyć stanowi jedno z kluczowych wyzwań współczesnego sektora finansowego, zarówno w Polsce, jak i na świecie. Rosnąca złożoność otoczenia gospodarczego, dynamiczny rozwój technologii oraz zmieniające się techniki działania przestępców sprawiają, że instytucje finansowe muszą konsekwentnie udoskonalać narzędzia i strategie minimalizacji ryzyka. Celem poniższego rozdziału jest przedstawienie aktualnej skali nadużyć, identyfikacja najważniejszych trendów oraz wskazanie wyzwań, z jakimi mierzą się instytucje finansowe.

Aby ocenić skalę zjawiska nadużyć, podobnie jak w ubiegłych latach, zapytaliśmy respondentów o ich ocenę zmiany intensywności występowania zjawiska nadużyć w ciągu ostatniego roku. Uzyskane wyniki wskazują na utrzymujące się wyzwania w tym obszarze, co zaprezentowaliśmy na wykresie 3.

W okresie między 2022 a 2024 rokiem odsetek respondentów dostrzegających wzrost liczby nadużyć nie przekraczał 40%. Tych, którzy w tym okresie uznawali, że sytuacja się nie zmieniła, było około 50%, z kolei poprawę sytuacji obserwowano u 8–12,5% badanych. Tegoroczne wyniki wyraźnie wskazują, że problem nadużyć dotknął większej części podmiotów rynku finansowego. Blisko połowa badanych instytucji wskazała na wzrost liczby nadużyć. Według 43% respondentów intensywność zjawiska nadużyć nie zmieniła się w stosunku do ubiegłego roku, a 10% wskazało, że nadużyć było mniej.

**Wykres 3.** Zmiana intensywności występowania zjawiska nadużyć w ciągu ostatnich 12 miesięcy względem poprzedniego roku (porównanie edycji z lat 2022–2025)

Źródło: ZPF/EY.



Wzrost liczby nadużyć może być związany z coraz powszechniejszym wykorzystaniem środowiska cyfrowego przez przestępców, w którym oszustwa są prostsze i tańsze do popełnienia. Zostało to szerzej omówione w dalszej części raportu.

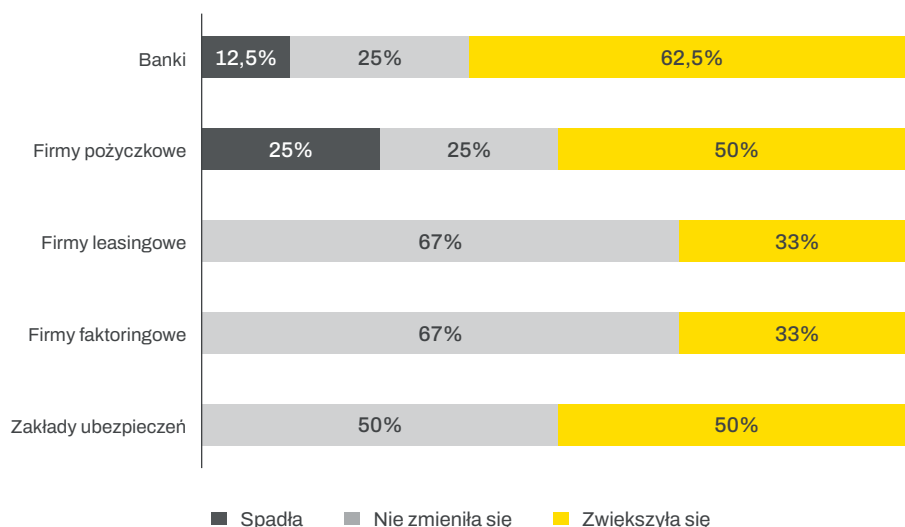
Analiza dynamiki zjawiska nadużyć w poszczególnych sektorach rynku finansowego wskazuje na zróżnicowane postrzeganie skali ryzyka w zależności od rodzaju instytucji. Przedstawiony na wykresie 4 rozkład odpowiedzi wyraźnie pokazuje, że niepokojący trend wzrostowy koncentruje się w niektórych sektorach. Różnice pomiędzy poszczególnymi branżami wskazują na potrzebę wdrażania indywidualnych strategii zarządzania ryzykiem nadużyć.

W sektorze leasingowym większość, bo aż 67% respondentów, uznała, że intensywność nadużyć w ostatnim roku nie uległa istotnym zmianom. Wzrost skali problemu zaobserwowało 33% przedstawicieli tego sektora i jednocześnie żaden z nich nie odnotował spadku liczby incydentów. Podobne obserwacje wynikają z odpowiedzi udzielonych przez przedstawicieli sektora faktoringowego.

Odpowiedzi respondentów z sektora ubezpieczeniowego były zbliżone do tych z branży leasingowej i faktoringowej. Eksperti podkreślają, że w ostatnich latach wzrosła świadomość przestępczości ubezpieczeniowej oraz zaangażowanie instytucji w działania prewencyjne, szczególnie w obszarze ubezpieczeń majątkowych, gdzie wymiana informacji jest coraz powszechniejsza. Dostrzegalne są także różnice w intensywności działań pomiędzy poszczególnymi działami ubezpieczeń – w działach ubezpieczeń na życie aktywność prewencyjna jest mniej intensywna niż w przypadku ubezpieczeń majątkowych. Eksperti wskazują, że poziom nadużyć pozostaje podobny, choć zmieniają się metody sprawców.

**Wykres 4.** Zmiana intensywności występowania zjawiska nadużyć w ciągu ostatnich 12 miesięcy względem poprzedniego roku – podział na sektory objęte badaniem

Źródło: ZPF/EY.



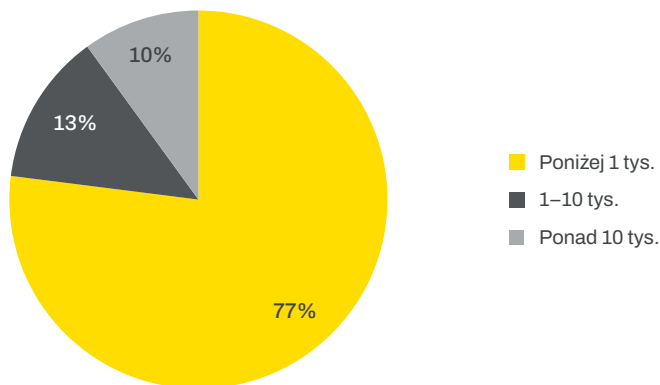
Zarówno dane pochodzące z przeprowadzonego badania ankietowego, jak i opinie ekspertów zebrane podczas wywiadów, wskazują, że kluczowym zjawiskiem pozostaje rosnąca skala nadużyć opartych na socjotechnice. Pomimo zwiększonych wysiłków po stronie instytucji finansowych, liczba tego typu incydentów nie maleje. Zauważono, że rozwój nowych technologii ułatwia działania przestępcze – zarówno pod względem kosztów, jak i dostępności. Wskazano, że jeszcze kilka lat temu wykorzystanie spoofingu, czyli techniki polegającej na podszywaniu się pod zaufany numer telefonu (np. infolinię banku), wiązało się z wysokim kosztem jednostkowym. Obecnie tego typu narzędzia są tanie i powszechnie dostępne, co zwiększa skalę ich wykorzystania przez przestępców.

W osobnym pytaniu w ankiecie poproszono respondentów o wskazanie, ile prób nadużyć zostało zidentyfikowanych w ich instytucjach w badanym okresie (wykres 5). Wyniki pokazują, że w większości organizacji liczba prób nadużyć w 2024 roku nie przekraczała 1 tys. Sytuacja ta dotyczy 77% respondentów. Zaobserwowano, że taki poziom liczby prób nadużyć zadeklarowały instytucje relatywnie mniejsze w grupie respondentów, czyli te, które na koniec 2024 roku obsługiwały mniej niż 100 tys. klientów. Do grona tych firm należeli przedstawiciele każdego sektora.

Tylko 13% instytucji wskazało, że w badanym okresie liczba prób nadużyć mieściła się w przedziale od 1 tys. do 10 tys. Z takim poziomem zagrożenia mierzyli się przedstawiciele większych (powyżej 80 tys. aktywnych klientów) firm pożyczkowych, banków oraz firm leasingowych. Odsetek respondentów, którzy zadeklarowali ponad 10 tys. prób nadużyć w swoich organizacjach, wynosi 10%. Najczęściej z taką skalą zjawiska miały do czynienia instytucje leasingowe oraz banki. Patrząc na wielkość instytucji, do grupy z największą liczbą prób nadużyć należały wyłącznie podmioty z bazami liczącymi ponad 3 miliony aktywnych klientów.

**Wykres 5.** Liczba prób nadużyć w branży finansowej

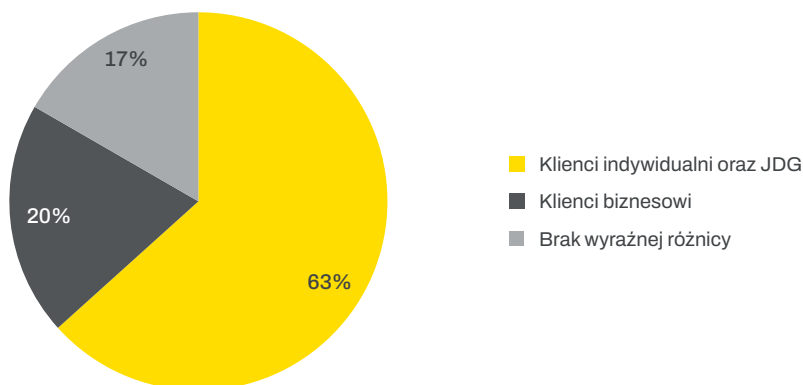
Źródło: ZPF/EY.



W tegorocznej edycji badania uwzględniono również pytanie o to, jakie grupy klientów, według opinii przedstawicieli instytucji finansowych, najczęściej są ofiarami działań przestępczych (wykres 6). Aż 63,3% respondentów wskazało, że są to klienci indywidualni oraz jednoosobowe działalności gospodarcze. Warto zauważyć, że jedynie 20% wszystkich ankietowanych wskazało klientów biznesowych jako grupę bardziej narażoną na ryzyko nadużyć, natomiast 16,7% respondentów nie dostrzegło istotnych różnic pomiędzy analizowanymi kategoriami. Może to świadczyć o tym, że klienci indywidualni oraz mikroprzedsiębiorstwa, ze względu na ograniczoną skalę działalności, mniejsze zasoby oraz niższą świadomość zagrożeń, są mniej przygotowani do skutecznego rozpoznawania i przeciwdziałania próbom nadużyć, co przekłada się na ich wyższą podatność na działania przestępcze.

**Wykres 6.** Grupy klientów najbardziej narażone na ryzyko nadużyć w badanym okresie

Źródło: ZPF/EY.



Biorąc pod uwagę poszczególne typy instytucji objęte badaniem, respondenci z sektora bankowego, faktoringowego, pożyczkowego i ubezpieczeniowego najczęściej wskazywali, że najbardziej podatni na zagrożenia są klienci indywidualni oraz jednoosobowe działalności gospodarcze. W sektorze leasingowym z kolei ponad połowa ankietowanych wskazała jako najbardziej narażone podmioty biznesowe, co wynika ze specyfiki oferty firm leasingowych skierowanej głównie do przedsiębiorstw.

W analizie uwzględniono także wypowiedzi ekspertów na temat najważniejszych wyzwań praktycznych w tym obszarze. Wskazują oni, że klienci indywidualni są szczególnie narażeni na nadużycia z powodu braku formalnych mechanizmów zabezpieczających, powszechnie stosowanych w relacjach z klientami instytucjonalnymi. Jednocześnie zwracają uwagę, że mniejsze przedsiębiorstwa, zwłaszcza o charakterze rodzinnym, mogą być podatne na działania socjotechniczne, takie jak spoofing czy podszywanie się pod osoby zarządzające.

Eksperti zaakcentowali również istotną lukę edukacyjną, zwłaszcza wśród młodzieży, która, uzyskując dostęp do kont bankowych, bywa wykorzystywana jako tzw. muły finansowe, które świadomie lub nieświadomie uczestniczą w procederze prania pieniędzy lub transferu środków pochodzących z przestępstw. Nasi rozmówcy wskazują, że działania edukacyjne powinny być kierowane zarówno do młodych użytkowników, jak i ich rodzin, a kampanie społeczne wymagają nowego podejścia, ponieważ obecnie bywają postrzegane jako nieangażujące lub pozbawione wiarygodności. W toku wywiadów eksperci zwrócili ponadto uwagę na to, że to właśnie nieświadomość klienta, brak reakcji na niepokojące sygnały oraz skłonność do ponownego ulegania tym samym schematom socjotechnicznym znacząco zwiększają skuteczność prób nadużyć i utrudniają instytucjom finansowym w przeciwdziałaniu nadużyciom.

Przeważająca większość (90%) uczestników tegorocznego badania stwierdziła, że problem nadużyć nie maleje. Aby lepiej zrozumieć podłoże tego stwierdzenia, w osobnym pytaniu poprosiliśmy o wskazanie poziomu ryzyka występowania poszczególnych rodzajów nadużyć z badanego okresu (wykres 7). W odpowiedziach wykorzystana została 5-stopniowa skala, gdzie „1” oznacza niski poziom zagrożenia danym rodzajem nadużycia, a „5” – bardzo wysoki.

Z udzielonych odpowiedzi wynika, że, tak samo jak w roku ubiegłym, to wyłudzenia produktów kredytowych (średnia ocena 3,7) są postrzegane jako jedno z bardziej znaczących zagrożeń. Potwierdzają to dane z raportu infoDOK<sup>1</sup>, zgodnie z którymi w pierwszym kwartale 2025 roku próby wyłudzeń kredytów osiągnęły łączną wartość aż 97,2 mln zł, co oznacza wzrost o ponad 17% w porównaniu z rokiem poprzednim. Dodatkowo, autorzy tego raportu wskazują, że średnio co 35 minut dochodzi do wyłudzenia kredytu. Rzeczywista skala problemu może być jednak nieporównywalnie większa, ponieważ nie każda próba wyłudzenia jest identyfikowana i rejestrowana.

Równie wysoko (3,6) zostało ocenione przeszacowanie wartości przedmiotu leasingu. Podobne wyniki dotyczą też wyłudzeń z użyciem kart płatniczych (3,2) i działań klientów wynikających z wiedzy o procesach transakcyjnych, np. friendly fraud czy family fraud (3,2). Family fraud to forma nadużycia finansowego, w której osoba blisko spokrewniona lub pozostająca w relacji z ofiarą wykorzystuje jej dane osobowe lub dostęp do instrumentów finansowych w celu dokonania nieautoryzowanej transakcji. Jednym z rodzajów tego typu nadużycia są tzw. romance fraud, na które wskazuje raport *Internet Organised Crime Threat Assessment 2024*. W tego typu

<sup>1</sup> Raport InfoDOK. I kwartał 2025, Związek Banków Polskich, Warszawa 2025.

naduźciach oszuści budują relację emocjonalną z ofiarą, aby zdobyć jej zaufanie i ostatecznie doprowadzić do wyłudzenia pieniędzy. Według raportu, coraz częściej wykorzystywane są w tym celu narzędzia sztucznej inteligencji, które umożliwiają dotarcie do większej liczby osób jednocześnie oraz skuteczniejsze manipulowanie emocjami. AI pozwala na tworzenie przekonujących profili, wiadomości czy nawet głosów i obrazów, co zwiększa skuteczność oszustw i utrudnia ich wykrycie<sup>2</sup>.

Nieautoryzowane transakcje na rachunkach, związane z przejściem dostępu do konta, również osiągnęły średnią ocenę 3,2. Ten aspekt wpisuje się w treść raportu *Annual Fraud Report 2025*, gdzie autorzy wskazują, że coraz większym problemem są te same transakcje, nazwane tam Authorised Push Payment (APP)<sup>3</sup>. W tego rodzaju fraudach ofiara, zmanipulowana przez przestępcę podszywającego się pod zaufany podmiot, sama autoryzuje przelew na rzecz oszusta. To kolejny typ przestępstw oparty na inżynierii społecznej, która ewoluuje i przenika do systemów finansowych, powodując znaczne straty zarówno dla instytucji, jak i klientów.

**Wykres 7.** Zagrożenie wystąpienia poszczególnych rodzajów nadużyć w instytucjach finansowych

Średnia z ocen w skali 1–5, gdzie „1” oznacza zagrożenie nieistotne, a „5” – bardzo istotne

Źródło: ZPF/EY.



Inaczej postrzegane będą schematy nadużyć, które mogą materializować się tylko w niektórych typach instytucji. Kradzież przedmiotu leasingu oraz sprzedaż przedmiotu leasingu należącego do firmy leasingowej uzyskały średnią ocenę 2,9, co zaskakująco wskazuje na umiarkowane postrzeganie ryzyka. Eksperti w wywiadach podkreślili jednak, że obecnie najczęściej dochodzi do nadużyć polegających na wielokrotnym leasingowaniu tego samego przedmiotu lub, wspomnianym wcześniej i ocenionym jako drugie najważniejsze ryzyko, przeszacowaniu jego wartości. Oba

<sup>2</sup> Internet Organised Crime Threat Assessment (IOCTA) 2024, Europol 2024, Publications Office of the European Union.

te zjawiska stanowią istotne wyzwanie dla sektora leasingowego, szczególnie, że często dotyczą specjalistycznych maszyn i urządzeń, których wartość jest trudna do oceny bez posiadania branżowej ekspertyzy.

W ramach badania umożliwiliśmy również respondentom wskazanie innych schematów nadużyć lub zagrożeń, które nie zostały uwzględnione we wcześniejszych pytaniach. W odpowiedziach pojawiały się podobne przykłady schematów. Wśród najczęściej wskazywanych zagrożeń znalazły się nadużycia związane z tożsamością, w tym kradzież danych osobowych oraz oszustwa oparte na socjotechnice. Respondenci zauważyli, że oszuści często wykorzystują manipulację, aby zdobyć poufne informacje, co prowadzi do poważnych konsekwencji zarówno dla instytucji, jak i ich klientów. Przykładem fraudów wykorzystujących socjotechnikę są tzw. oszustwa inwestycyjne. Zgodnie z danymi z *Raportu rocznego CSIRT KNF w 2024 roku* zidentyfikowano i zgłoszono prawie 46 tys. domen powiązanych z fałszywymi inwestycjami. Stanowiło to blisko 90% wszystkich domen zgłoszonych do zespołu reagowania na incydenty komputerowe działającego przy Komisji Nadzoru Finansowego. Oszustwa inwestycyjne polegają na celowym wprowadzaniu ofiar w błąd w celu wyłudzenia pieniędzy, najczęściej poprzez obiecywanie wysokich zysków z fałszywych lub nieistniejących inwestycji (np. w kryptowaluty, akcje, nieruchomości, startupy), przy jednoczesnym ukrywaniu ryzyka lub prawdziwej natury przedsięwzięcia. Coraz powszechniejsze stają się reklamy generowane przez AI, które mają przyciągać ofiary, a mając na względzie rozwój sztucznej inteligencji ten trend będzie się nasilał. Także oszustwa bankowe są wskazywane przez respondentów jako jedne z częściej stosowanych przez przestępców technik. Mogą polegać zarówno na podszyciu się pod pracownika banku, jak i podszywaniu się pod bank czy inną instytucję finansową (phishing)<sup>4</sup>. Zgodnie z raportem *IOCTA 2024*, phishing pozostaje najczęściej wykorzystywanym wektorem ataku w cyberprzestępczości w Unii Europejskiej<sup>5</sup>. Potwierdza to także KNF, która w swoim raporcie za 2024 rok wskazuje, że liczba incydentów phishingowych wzrosła niemal czterokrotnie w porównaniu z rokiem 2021. Tylko w 2024 roku zgłoszono 51 241 domen phishingowych. Dane te wskazują na rosnącą skalę zagrożenia i potwierdzają potrzebę zdecydowanych działań ze strony instytucji finansowych oraz organów nadzorczych. W ostatnich latach szczególną popularnością cieszył się także smishing (phishing SMS-owy), a nowym zagrożeniem stał się quishing, czyli ataki z użyciem fałszywych kodów QR.

Kolejną istotną kategorią były oszustwa związane z leasingiem i finansowaniem. Respondenci wskazali na problemy takie jak przewartościowanie pojazdów oraz fałszowanie dokumentacji finansowej. W przypadku leasingu, zafałszowane dane skutkują błędną oceną ryzyka transakcji, co przekłada się na decyzje finansowe obciążone wysokim prawdopodobieństwem niewypłacalności klienta. To z kolei może wygenerować straty – zarówno w postaci utraconych należności, jak i kosztów odzyskiwania przedmiotu leasingu oraz obsługi windykacyjnej.

Przedstawiciele branży ubezpieczeniowej wskazali natomiast na wyłudzenie usług, np. oferowanie pojazdów zastępczych. W takim scenariuszu klienci starają się uzyskać korzyści finansowe w sytuacjach, w których nie doszło do żadnej szkody.

Tytułem uzupełnienia wyników ankiety, podczas wywiadów eksperci zostali poproszeni o wskazanie przykładów nadużyć, które napotykają w codziennej praktyce. Celem było zidentyfikowanie niestandardowych metod, które mogą nie mieścić się

<sup>4</sup> *Raport Roczny CSIRT KNF 2024, KNF 2024.*

<sup>5</sup> *Internet Organised Crime Threat Assessment (IOCTA) 2024, op.cit.*

w typowych kategoriach klasyfikacyjnych. Wśród przykładów wskazano m.in. próby zastąpienia wymaganych dokumentów – takich jak umowa czy faktura – innymi, jak np. niepowiązany paragon w języku arabskim czy rzekoma umowa przewozowa po japońsku, która okazała się warunkiem gwarancji sprzętu RTV.

Podobnie jak w poprzednich latach, w odniesieniu do identyfikowanych zagrożeń respondenci zostali poproszeni o dokonanie oceny, jak dobrze ich instytucje są przygotowane do reagowania na poszczególne ich rodzaje (wykres 8). W odpowiedziach wykorzystana została pięciostopniowa skala, gdzie „1” oznaczał niski poziom przygotowania do reagowania na dany rodzaj nadużycia, a „5” – bardzo wysoki.

**Wykres 8.** Poziom przygotowania instytucji finansowych do reagowania na różne rodzaje nadużyć

Średnia z ocen w skali 1–5, gdzie „1” oznacza słabe przygotowanie, a „5” – bardzo dobre przygotowanie

Źródło: ZPF/EY.



Badane instytucje najlepiej oceniają swoje przygotowanie do przeciwdziałania dwóm rodzajom nadużyć. Na pierwszym miejscu znalazły się wyłudzenia z wykorzystaniem kart płatniczych (4,1). Może to świadczyć o skuteczności wdrożonych zabezpieczeń oraz efektywnym działaniu procedur detekcyjnych. Na drugim miejscu respondenci wskazali wyłudzenia kredytów i pożyczek (4,0), które, mimo że są najpowszechniej występującym typem nadużyć, stanowią obszar, w jakim instytucje czują się dobrze przygotowane. Wyniki tegorocznego badania są zbieżne z danymi pochodzącymi ze wspomnianego raportu InfoDOK, wskazującymi, że w 2024 roku udało się udaremnić 13 009 prób wyłudzeń kredytów na łączną kwotę 338,5 mln zł<sup>6</sup>.

Relatywnie dobrze respondenci ocenili również swoje przygotowanie na nadużycie polegające na działaniu klienta wynikającym z wiedzy o procesach transakcyjnych, czyli tak zwanych friendly fraud / family fraud. W tym przypadku instytucje oceniły

<sup>6</sup> Raport InfoDOK. I kwartał 2025, op.cit.

swoje przygotowanie średnio na 3,7. Nieautoryzowane transakcje na rachunkach oraz podanie nieprawdziwych okoliczności zaistnienia szkody to obszary, w których instytucje czują się mniej pewnie, z ocenami odpowiednio 3,7 i 3,2. W kontekście leasingu, kradzież przedmiotu leasingu oraz sprzedaż przedmiotu leasingu należącego do firmy leasingowej to obszary, które wymagają szczególnej uwagi – uzyskały odpowiednio średnią na poziomie 3,4 oraz 2,9.

Pozyskane w ramach przeprowadzonych wywiadów wypowiedzi eksperckie wskazują, że poziom przygotowania instytucji finansowych do przeciwdziałania nadużyciom jest mocno zróżnicowany – zarówno pod względem dostępnych zasobów technologicznych, jak i dojrzałości organizacyjnej. Przedstawiciele większych podmiotów, w szczególności zakładów ubezpieczeń, podkreślali rolę zaawansowanych rozwiązań technologicznych stosowanych w detekcji nadużyć. Jednocześnie zwracano uwagę, że nie wszystkie podmioty sektora dysponują takimi możliwościami – część instytucji wciąż opiera się na prostych narzędziach analitycznych, takich jak scoring w arkuszach kalkulacyjnych czy manualne przeglądanie transakcji w celu identyfikacji nietypowych zachowań.

Podczas rozmów z przedstawicielami sektora finansowego zapytano również o to, które elementy systemu przeciwdziałania nadużyciom są najskuteczniejsze. Eksperci najczęściej wskazywali, że najmocniejszą stroną są pracownicy – osoby dobrze przeszkolone, świadome ryzyka związanego z nadużyciami i potrafiące rozpoznawać sygnały ostrzegawcze. Uwagę zwracali też na znaczenie odpowiednio wdrożonych rozwiązań technologicznych, które w połączeniu z wiedzą ekspercką umożliwiają holistyczne podejście do zarządzania incydentami. W sektorze bankowym dodatkową przewagą stanowi możliwość formalnej i uregulowanej prawnie wymiany informacji pomiędzy instytucjami, co pozwala szybciej identyfikować znane schematy oszustw i ograniczać ich skutki. Rozmówcy podkreślili również, jak istotna jest elastyczność organizacyjna. Instytucje deklarowały wzmocnianie swoich zespołów, dostosowywanie struktur oraz podłączanie nowych baz danych, aby skuteczniej reagować na ewoluujące zagrożenia.

Aby lepiej zrozumieć perspektywę uczestników badania, przeanalizowano także zagrożenia przypisywane poszczególnym kanałom dystrybucji produktów i usług finansowych. W osobnym pytaniu respondenci zostali poproszeni o ocenę istotności zagrożeń występujących w poszczególnych kanałach dystrybucji produktów i usług finansowych, na podstawie doświadczeń z 2024 roku (wykres 9). Do każdego kanału należało przypisać ocenę w pięciostopniowej skali, gdzie 1 oznaczało mało istotne zagrożenie, a 5 – bardzo istotne.

Kanał online oraz kanał mobilny uzyskały najwyższą średnią ocenę na poziomie odpowiednio 4,1 i 3,9, co sugeruje, że są postrzegane jako najbardziej narażone na zagrożenia. Wysoka ocena może być związana z rosnącą liczbą cyberataków oraz problemami z bezpieczeństwem danych w sieci. Niewiele niższą ocenę (3,3) otrzymały dwa kanały tradycyjne, czyli oddziały własne lub pośrednicy/agenci oraz kanał telefoniczny. Kanały te, zdaniem respondentów, są mniej ryzykowne niż kanały cyfrowe, co wskazuje, że nadal bezpośredni kontakt z klientem ma duże znaczenie dla ograniczenia ryzyka wystąpienia nadużyć.

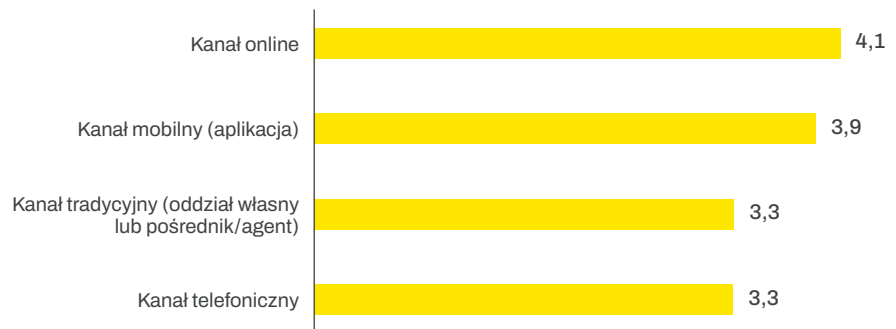
Przedstawiciele instytucji finansowych, z którymi przeprowadzono wywiady, potwierdzili, że kanał dystrybucji odgrywa istotną rolę w strategiach przestępców i może wpływać na podatność instytucji na określone typy nadużyć. Rozmówcy zwrócili uwagę, że oszuści coraz częściej wykorzystują znajomość specyfiki modeli sprzedażowych poszczególnych firm – potrafią rozróżnić, które zakłady ubezpieczeń

funkcjonują głównie w modelu agencyjnym, a które oferują produkty w modelu direct. To pozwala im koncentrować się na tych instytucjach, których procedury są mniej restrykcyjne lub bardziej podatne na manipulacje. Eksperti podkreślili też dynamiczny rozwój kanałów cyfrowych, zarówno webowych, jak i mobilnych. Zauważyli, że chociaż aplikacje mobilne często oferują lepsze zabezpieczenia, takie jak powiązanie z konkretnym urządzeniem, to nadal są popularnym celem ataków z uwagi na rosnącą liczbę użytkowników.

**Wykres 9.** Istotność zagrożeń występujących w poszczególnych kanałach dystrybucji produktów i usług finansowych

Średnia z ocen w skali 1–5, gdzie „1” oznacza zagrożenie nieistotne, a „5” – bardzo istotne

Źródło: ZPF/EY.



Kluczowe znaczenie ma również jakość wdrożeń technologicznych oraz odpowiednie przeszkolenie pracowników, którzy mogą zareagować na próby oszustwa na wczesnym etapie. Z perspektywy długofalowej eksperci zauważyli, że zarówno tradycyjne kanały, szczególnie w przypadku klientów korporacyjnych oczekujących kontaktu z doradcą, jak i zdalne, preferowane przez klientów detalicznych, będą się utrzymywać. W ocenie ekspertów przestępcy nie ograniczają się do jednego kanału, a raczej testują różne ścieżki w zależności od poziomu zabezpieczeń i reakcji personelu. Takie podejście wymaga od instytucji finansowych szerokiego zarządzania ryzykiem, które uwzględni złożoność i różnorodność modeli dystrybucji.

## Narzędzia przeciwdziałania nadużyciom

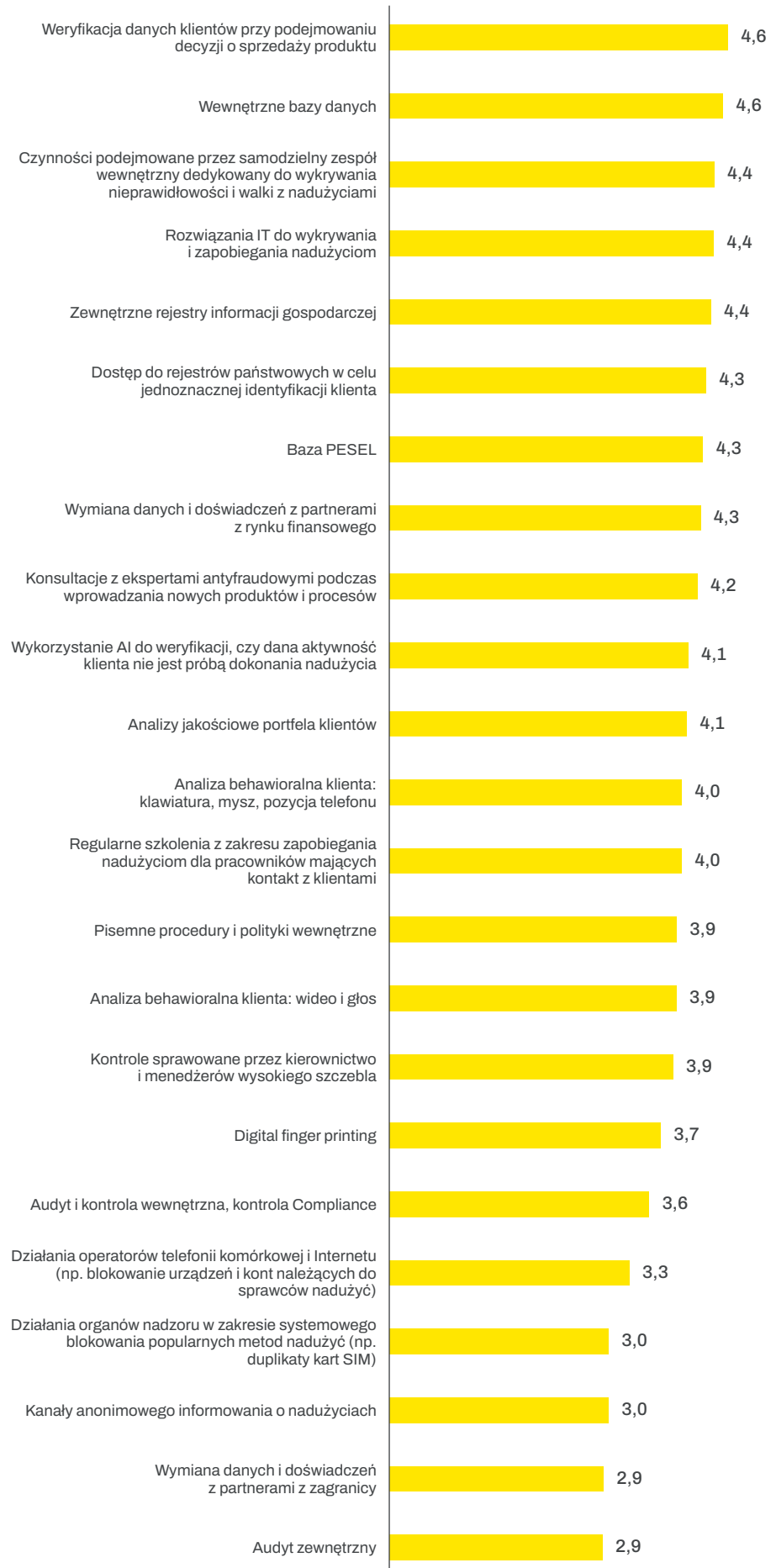
Metody nadużyć zmieniają się w sposób dynamiczny, co wymaga od instytucji finansowych wdrożenia elastycznych i kompleksowych strategii przeciwdziałania. W tej części badania podjęliśmy próbę zidentyfikowania kluczowych wyzwań w tym zakresie. Poprosiliśmy respondentów o ocenę skuteczności poszczególnych metod walki z nadużyciami, które są stosowane w ich instytucjach (w skali od 1 do 5, gdzie „1” oznacza, że dana metoda jest nieskuteczna, a „5” – bardzo skuteczna) bądź tych, które nie są stosowane (w tym przypadku respondenci mogli ocenić metodę jako potencjalnie pomocną bądź nieprzydatną). Analiza odpowiedzi pozwoliła zidentyfikować rozwiązania postrzegane jako najbardziej efektywne oraz te, które pozostają wśród respondentów mniej popularne lub niedostępne (wykresy 10 i 11).

Najwyższy poziom skuteczności przypisano metodom o charakterze prewencyjnym, narzędziom silnie zintegrowanym z codziennymi procesami, wspierającym bieżące wykrywanie i zapobieganie nadużyciom. Na czele znalazła się weryfikacja danych klientów przy podejmowaniu decyzji sprzedażowych (ze średnią oceną 4,6) oraz wewnętrzne bazy danych (4,6). Wysoko oceniono również działania wyspecjalizowanych wewnętrznych zespołów antyfraudowych oraz rozwiązania IT wspierające wykrywanie i zapobieganie nadużyciom (obie metody po 4,4).

**Wykres 10.** Skuteczność metod walki z nadużyciami, które są wykorzystywane w badanych instytucjach

Średnia z ocen w skali 1–5, gdzie „1” oznacza metodę nieskuteczną, a „5” – bardzo skuteczną

Źródło: ZPF/EY.



W dolnej części hierarchii ocenianych rozwiązań znalazły się kanały anonimowego informowania o nadużyciach oraz działania organów nadzoru ukierunkowane na systemowe blokowanie popularnych metod nadużyć takich jak duplikaty kart SIM (oba z tą samą średnią oceną 3,0). Z kolei najniższe noty – po 2,9 – uzyskały: wymiana danych i doświadczeń z partnerami z zagranicy oraz audyt zewnętrzny (2,9). Należy tu zaznaczyć, że audyt zewnętrzny oceniano jedynie z perspektywy jego skuteczności w detekcji nadużyć.

Warto nadmienić, że jedynie cztery ze wszystkich wymienionych w pytaniu metod są wykorzystywane w każdej z badanych instytucji. Są to: weryfikacja danych klientów przy podejmowaniu decyzji o sprzedaży produktu oraz wewnętrzne bazy danych (w obu przypadkach ocenione na 4,6), zewnętrzne rejestry informacji gospodarczej (4,4) oraz pisemne procedury i polityki wewnętrzne (3,9).

Odnosząc się do „wymiany danych i doświadczeń z partnerami z zagranicy”, w przeprowadzonych wywiadach jeden z naszych rozmówców wskazał na istotne ograniczenia infrastrukturalne, które utrudniają sprawną wymianę informacji między instytucjami. W jego ocenie, pomimo rosnących zagrożeń oraz postępującej cyfryzacji, niektóre sektory nadal opierają wymianę danych antyfraudowych na niewydolnych rozwiązaniach, takich jak e-mail. Brak zintegrowanych, bezpiecznych systemów komunikacji może istotnie wpływać na opóźnienia w reagowaniu na incydenty oraz ograniczać skuteczność współpracy między podmiotami rynku.

Z kolei w przypadku kanału anonimowego zgłaszania nadużyć, który uzyskał jedną z najniższych ocen w naszej analizie (3,0), warto zauważyć, że funkcjonuje on w aż 80% instytucji objętych badaniem. Dla porównania, dane zawarte w międzynarodowym raporcie *ACFE Occupational Fraud 2024*<sup>7</sup> pokazują, że aż 43% przypadków nadużyć zostało wykrytych dzięki zgłoszeniom – ponad trzykrotnie częściej niż przy wykorzystaniu jakiegokolwiek innej metody. Co istotne, ponad połowa tych sygnałów pochodziła od pracowników, a kolejne 32% – od klientów i kontrahentów. Zestawienie tych dwóch źródeł pokazuje wyraźnie, że kanały anonimowego zgłaszania nieprawidłowości, chociaż ogólnie są potężnym narzędziem, w Polsce nie pełnią istotnej roli. Nasuwającym się wnioskiem jest to, że popularyzacja kanałów oraz ich odpowiedniego ustrukturyzowania wśród polskiego społeczeństwa mogłaby znacząco zwiększyć wykrywalność nadużyć. Zgodnie z opiniami ekspertów, którzy w toku wywiadów podzielili się obserwacjami dotyczącymi funkcjonowania kanałów whistleblowingowych, skuteczność tych narzędzi zależy w dużej mierze od dwóch czynników: wiarygodności procesu i poziomu zaufania pracowników. Eksperti zwracają uwagę na konieczność wdrażania rozwiązań technologicznych, które zapewniają pełną anonimowość i bezpieczeństwo zgłaszających, a także na potrzebę rzetelnego, instytucjonalnego podejścia do analizy każdej zgłoszonej sprawy. Jednocześnie podkreślają, że sama obecność kanału nie wystarcza – kluczowe znaczenie ma komunikacja wewnętrzna oraz budowanie świadomości, że każde zgłoszenie jest realnie analizowane i może skutkować zmianą procesów lub działań naprawczych. Rozmówcy wskazują również, że rozwój kultury organizacyjnej wspierającej sygnalistów (whistleblowerów) wciąż znajduje się we wczesnej fazie, jednak z biegiem czasu ten mechanizm będzie zyskiwał na znaczeniu jako narzędzie doskonalenia wewnętrznych procedur i eliminowania słabych punktów systemu.

<sup>7</sup> *Occupational Fraud 2024: A Report to the Nations*, ACFE 2024.

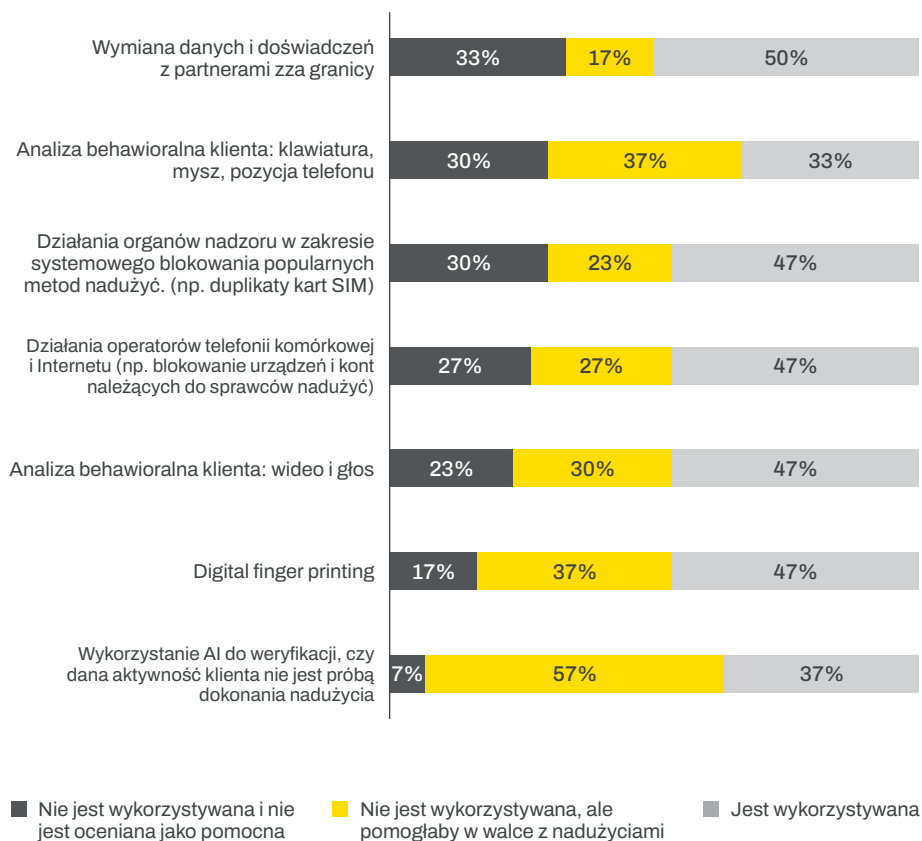
Eksperti uczestniczący w wywiadach zostali również zapytani o priorytety inwestycyjne instytucji finansowych w zakresie walki z nadużyciami – czy skupiają się one na rozwijaniu już posiadanych rozwiązań, czy też poszukują nowych metod przeciwdziałania. W odpowiedziach dominowało wyważone podejście, zakładające zarówno wzmacnianie istniejących systemów, jak i wdrażanie innowacyjnych technologii, w tym narzędzi opartych na uczeniu maszynowym. Zwrócono uwagę, że nie wszystkie potrzeby wymagają nowych nakładów finansowych – równie istotna może być rozbudowa wewnętrznych struktur i dostosowywanie aktualnych narzędzi do zmieniających się schematów nadużyć. Jednocześnie podkreślano znaczenie współpracy wewnątrz grup kapitałowych oraz między instytucjami, zwłaszcza w sektorze bankowym, gdzie wymiana wiedzy operacyjnej stanowi istotny element budowania bezpieczeństwa całego rynku.

Wśród opinii ekspertów pojawiały się ponadto głosy podkreślające praktyczne znaczenie dobrze funkcjonujących kanałów whistleblowingowych. Zwracano uwagę, że nawet pojedyncze, anonimowe zgłoszenia – poddane właściwej analizie – mogą skutkować konkretnymi usprawnieniami organizacyjnymi, takimi jak uszczelnianie procedur, wprowadzanie zmian w zarządzaniu czy wzmacnianie nadzoru. Doświadczenia te pokazują, że mimo pewnych ograniczeń, kanały whistleblowingowe stanowią istotny element podnoszenia odporności instytucji na nadużycia.

Poza oceną skuteczności stosowanych metod walki z nadużyciami respondenci mieli możliwość oceny potencjalnej przydatności metod, które nie są wykorzystywane w ich instytucjach (wykres 11). Celem tej części badania było określenie potencjału wdrożeniowego poszczególnych rozwiązań w świetle aktualnych wyzwań operacyjnych. Uzyskane wyniki wskazują na wyraźnie rosnące zainteresowanie narzędziami opartymi na nowoczesnych technologiach.

**Wykres 11.** Metody walki z nadużyciami, które są bądź nie są wykorzystywane w badanych instytucjach

Źródło: ZPF/EY.



Największy odsetek odpowiedzi wskazujących, że dana metoda nie jest wykorzystywana, ale mogłaby pomóc, uzyskały: wykorzystanie sztucznej inteligencji do analizy aktywności klienta (57%), digital finger printing (37%) oraz zaawansowana analiza behawioralna (37%). Może to świadczyć o dostrzeżeniu przez sektor potencjału, jaki niosą ze sobą innowacje wspierające wykrywanie nadużyć w dynamicznie zmieniającym się środowisku cyfrowym.

Należy jednak podkreślić, że realizacja pełnego potencjału tych rozwiązań odbywa się w określonych ramach prawnych. Eksperti podkreślają, że choć sztuczna inteligencja może stanowić istotne wsparcie w przeciwdziałaniu nadużyciom, to aktualne przepisy ograniczają możliwości jej wykorzystania w sektorze finansowym. Szczególnym przykładem wskazanym przez jednego z rozmówców jest problematyka profilowania klienta, która w przypadku instytucji finansowych wiąże się z obowiązkiem uzyskania wyraźnej zgody na przetwarzanie danych w tym celu. Oznacza to konieczność spełnienia szeregu wymogów prawnych i organizacyjnych przed wdrożeniem skutecznych narzędzi analitycznych. Tymczasem przestępcy, działający poza ramami prawa, nie są ograniczeni takimi regulacjami – swobodnie gromadzą dane o potencjalnych ofiarach i wykorzystują je do tworzenia precyzyjnych profili, które ułatwiają skuteczne przeprowadzanie ataków.

W pytaniu dotyczącym metod walki z nadużyciami respondenci mieli również możliwość dodania własnych propozycji działań, których brakuje w ich organizacji, a mogłyby pomóc w przeciwdziałaniu nadużyciom. Wśród zgłoszonych przykładów pojawiły się m.in. potrzeba wykrywania podłączenia pulpitu zdalnego podczas sesji logowania oraz wykorzystanie płatnych narzędzi zewnętrznych, takich jak zaawansowane platformy online służące do prowadzenia dochodzeń i analiz w obszarze wykrywania oszustw finansowych.

Pomimo wyraźnego zainteresowania respondentów wdrażaniem nowoczesnych metod przeciwdziałania nadużyciom, istnieje szereg przeszkód w ich szerszym zastosowaniu w praktyce. Eksperti, z którymi przeprowadzono wywiady, wskazali na bariery takie jak wysokie koszty implementacji, brak mierzalnych efektów na wczesnym etapie, a także ograniczone zasoby technologiczne i kadrowe. Podkreślili również, wskazywane wcześniej w raporcie, znaczenie barier regulacyjnych – zwłaszcza w zakresie przetwarzania danych w środowiskach chmurowych oraz stosowania narzędzi opartych na sztucznej inteligencji. Nawet w sytuacji, gdy instytucje dysponują zaawansowanymi rozwiązaniami, ich praktyczne wykorzystanie bywa ograniczane ze względów bezpieczeństwa oraz ryzyka naruszenia przepisów. Dodatkowo rozmówcy zwrócili uwagę, że kluczową rolę w procesie decyzyjnym odgrywa postawa kadry zarządzającej – to właśnie świadomość i priorytety liderów organizacji w dużej mierze determinują, czy nowe metody rzeczywiście trafiają do praktyki operacyjnej.

W nawiązaniu do przedstawionych wcześniej obserwacji, kolejne pytanie ankiety zostało poświęcone identyfikacji najważniejszych problemów, z jakimi instytucje finansowe mierzą się w obszarze nadużyć (wykres 12). Analiza uzyskanych odpowiedzi pozwala nie tylko lepiej zrozumieć skalę wyzwań, przed jakimi stoją organizacje, ale także wskazuje na bariery, które utrudniają skuteczne zarządzanie ryzykiem nadużyć. Stanowi to istotny kontekst dla dalszej dyskusji na temat efektywności stosowanych rozwiązań oraz potrzeb rozwojowych sektora.

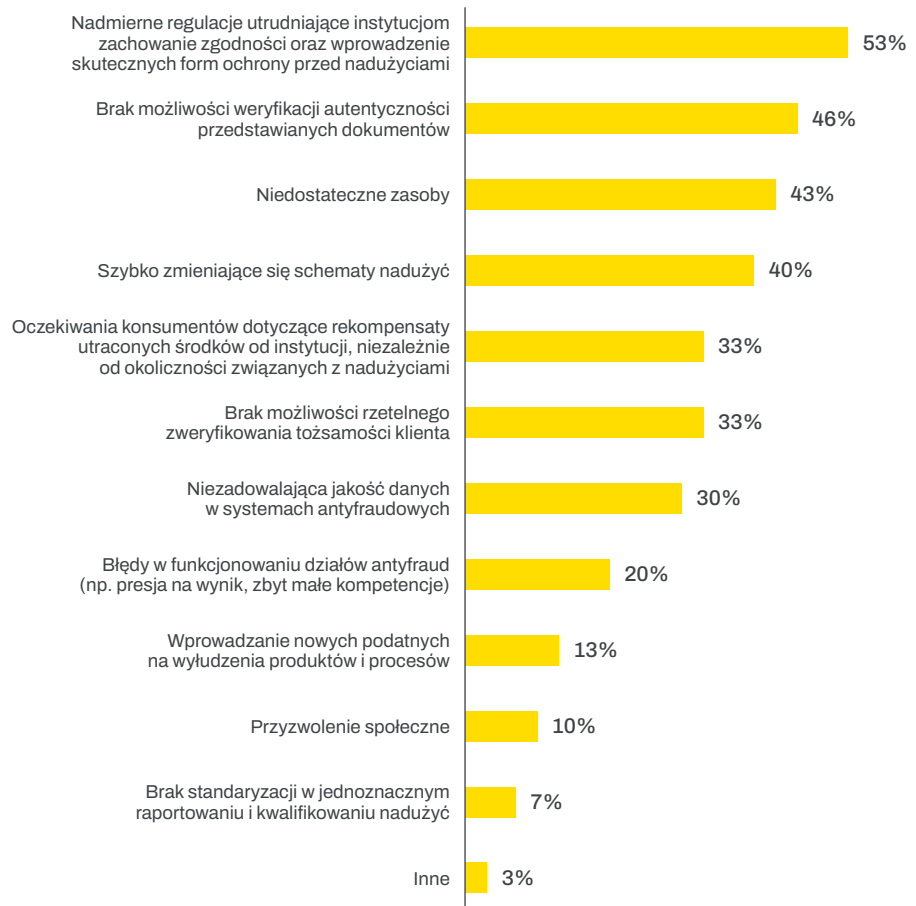
Zdaniem respondentów jednym z głównych problemów, z którym muszą się mierzyć instytucje finansowe, są zbyt skomplikowane przepisy i regulacje. Aż 53% osób biorących udział w badaniu wskazało, że przez nadmiar przepisów trudniej jest zachować zgodność z prawem i skutecznie bronić się przed nadużyciami. Z tego

powodu wprowadzanie nowych zabezpieczeń staje się bardziej skomplikowane, a instytucje muszą poświęcać wiele czasu oraz zasobów na dostosowanie się do wciąż zmieniających się wymagań.

W uzupełnieniu do wyników ankiety, problem nadmiernych regulacji jako istotnej bariery dla skutecznego przeciwdziałania nadużyciom został również szeroko poruszony w wywiadach przeprowadzonych z ekspertami. W swoich wypowiedziach wskazywali oni na rosnącą presję regulacyjną, która skutkuje powstawaniem rozproszonych i często niespójnych procedur wewnętrznych, znacząco utrudniających operacjonalizację procesów bezpieczeństwa. Zwracali też uwagę na potrzebę deregulacji, zwłaszcza w kontekście obszarów takich jak AML czy wykorzystanie sztucznej inteligencji, gdzie nadmiar wymagań formalnych ogranicza możliwości skutecznego działania. Nasi rozmówcy podkreślali, że instytucje finansowe, w odróżnieniu od przestępców, są zobowiązane do przestrzegania przepisów dotyczących m.in. profilowania klientów czy przetwarzania danych, co znacząco wpływa na ich zdolność do wdrażania nowoczesnych rozwiązań.

**Wykres 12.** Problemy, z jakimi zmagają się badane instytucje w obszarze nadużyć

Źródło: ZPF/EY.



Kolejnym istotnym zidentyfikowanym wyzwaniem jest brak możliwości weryfikacji autentyczności przedstawianych dokumentów, na który zwróciło uwagę 46% respondentów. W obliczu coraz bardziej wyrafinowanych metod oszustw ta kwestia staje się kluczowa dla skutecznej detekcji nadużyć. Warto zauważyć też, że 43% uczestników badania wskazało na niedostateczne zasoby, które ograniczają możliwości instytucji w zakresie walki z nadużyciami. Z kolei 40% respondentów podkreśliło

problem szybko zmieniających się schematów nadużyć, co utrudnia instytucjom dostosowanie się do nowych wyzwań. Wzrost innowacji w obszarze technologii finansowych stwarza nowe możliwości, ale jednocześnie rodzi nowe zagrożenia.

Wśród innych istotnych problemów znalazły się, wskazane przez 33% uczestników badania, oczekiwania konsumentów dotyczące rekompensaty utraconych środków od instytucji, niezależnie od okoliczności związanych z nadużyciami. Takie wyniki wskazują na rosnącą presję na instytucje finansowe, aby zapewniały ochronę swoich klientów. Również 33% respondentów zwróciło uwagę na brak możliwości rzetelnego zweryfikowania tożsamości klienta, co staje się kluczowe w dobie cyfryzacji i rosnącej liczby transakcji online.

W dalszej kolejności wśród analizowanych problemów znalazła się niezadowalająca jakość danych w systemach antyfraudowych (30% wskazań), co może wpływać na skuteczność działań w tym obszarze, czy też błędy w funkcjonowaniu działów antyfraud, takie jak presja na wyniki czy zbyt małe kompetencje pracowników (20%). Na dalszych miejscach znalazły się problemy związane z wprowadzaniem nowych, podatnych na wyłudzenia, produktów i procesów (13%) oraz z przyzwoleniem społecznym na nadużycia (10%), które mogą wpływać na postrzeganie tego zjawiska w społeczeństwie. Na końcu listy znajduje się, wskazany przez 7% uczestników badania, brak standaryzacji w jednoznacznym raportowaniu i kwalifikowaniu nadużyć, co podkreśla potrzebę ujednoczenia podejścia do tego problemu.

Biorąc pod uwagę uzyskane wyniki badania, można wnioskować, że instytucje finansowe stoją przed wieloma wyzwaniami w obszarze nadużyć, które wymagają kompleksowego podejścia oraz współpracy na różnych poziomach, aby skutecznie przeciwdziałać tym zagrożeniom.

## Nadużycia przyszłości, przyszłość nadużyć

Aby uzupełnić naszą analizę, postanowiliśmy zapytać respondentów o kluczowe zagrożenia, które mogą wpływać na rynek finansowy w ciągu najbliższych dwóch lat. Zostali oni poproszeni o ocenienie ryzyka wystąpienia danego zjawiska w skali od 1 (bardzo małe ryzyko) do 5 (bardzo duże ryzyko).

Wyniki w tym zakresie ujawniają niepokojące tendencje, które mogą znacząco wpłynąć na bezpieczeństwo sektora finansowego (wykres 13). Najistotniejsze ryzyka są powiązane z rozwojem i zastosowaniem sztucznej inteligencji. Tak samo jak w zeszłym roku, wśród najwyższej ocenianych zagrożeń wskazane zostały deep fake w zdalnych kanałach kontaktu (średnia ocena 3,9) oraz wykorzystanie AI do generowania nadużyć (3,9). Na niechlubnym podium znajduje się także wykorzystanie socjotechnik do manipulacji i oszustw (3,8) oraz wykorzystanie AI do generowania fałszywych tożsamości (3,8).

Na podstawie przeprowadzonych wywiadów z przedstawicielami instytucji finansowych, powyższe pytanie dotyczące prognozy zagrożeń w perspektywie najbliższych dwóch lat zostało jednoznacznie skorelowane z dynamicznym rozwojem technologii – zwłaszcza sztucznej inteligencji. Ekspertsi podkreślali, że nowe narzędzia, takie jak deep fake czy generatywne modele wykorzystywane do tworzenia fałszywych wizerunków, głosu lub treści, stają się coraz łatwiej dostępne i tańsze, co czyni je bardziej opłacalnymi z punktu widzenia przestępców. Zauważyli również rosnącą popularność fałszywych reklam publikowanych w mediach społecznościowych, tworzonych przy wsparciu AI, których celem jest pozyskiwanie danych klientów lub nakłanianie ich do wykonywania niekorzystnych transakcji.

**Wykres 13.** Kluczowe zagrożenia, które mogą wpłynąć na rynek finansowy w ciągu najbliższych dwóch lat

Średnia z ocen w skali 1–5, gdzie „1” oznacza zagrożenie bardzo małe, a „5” – bardzo duże

Źródło: ZPF/EY.



Odrębnym wątkiem wskazanym w wywiadach były wyzwania finansowe związane z rozbudową systemów antyfraudowych – szczególnie w mniejszych instytucjach, takich jak firmy leasingowe. Eksperti wskazywali, że brak środków na integrację z wieloma zewnętrznymi bazami danych oraz na rozwój nowych rozwiązań może znacząco osłabić poziom ochrony.

Warto również zwrócić uwagę na zagrożenie związane z modelami biznesowymi Fraud as a Service (FaaS) oraz Cybercrime as a Service (CaaS), które uzyskało średnią ocenę na 3,6. Zgodnie z raportem IOCTA 2024<sup>8</sup>, dynamicznie rozwija się także rynek phishing-as-a-service (PhaaS), który umożliwia nawet osobom bez wiedzy technicznej zamawianie fałszywych stron bankowych czy sklepów internetowych, przy czym kryptowaluty stanowią główną metodę płatności za tego typu usługi. Powszechne są także masowe kampanie tzw. „shock calls” łączące spoofing, socjotechnikę i call center.

<sup>8</sup> Internet Organised Crime Threat Assessment (IOCTA) 2024, op.cit.

Wśród zagrożeń, które plasują się tuż za najwyżej ocenianymi, znajdują się kwestie związane z wspomnianym już przeregulowaniem rynku finansowego oraz trudnościami powiązаныmi ze zgodnością z regulacjami, które, jak wskazano wcześniej w raporcie, nie mają zastosowania do przestępców. Problemy te, choć nie budzą tak intensywnych obaw jak inne ryzyka, sygnalizują potrzebę zmian systemowych. Z drugiej strony respondenci wskazują też na obniżenie standardów zabezpieczeń pod presją zwiększenia sprzedaży, uproszczenie procesów oraz poprawę doświadczeń klientów.

Wyniki badania jednoznacznie wskazują na rosnące obawy dotyczące nowoczesnych technologii oraz metod oszustw, które mogą zagrażać stabilności rynku finansowego. W obliczu tych wyzwań branża finansowa musi nieustannie dostosowywać swoje strategie zabezpieczeń do najnowszych odkryć w dziedzinie sztucznej inteligencji, z której przestępcy korzystają z dużą łatwością.

## Współpraca z organami ścigania

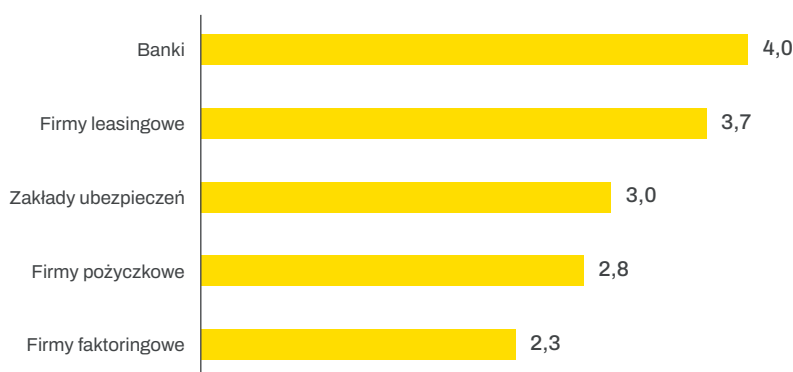
Współpraca sektora finansowego z organami ścigania odgrywa kluczową rolę w skutecznym przeciwdziałaniu rosnącym zagrożeniom i zapewnieniu bezpieczeństwa całego rynku. W ostatniej części badania respondenci zostali poproszeni o ocenę jakości tej współpracy, opierając się na doświadczeniach z 2024 roku. Odpowiedzi udzielano w skali od 1 do 5, gdzie 1 oznaczało bardzo słabą współpracę, a 5 – bardzo dobrą. Średnia ocena uzyskana ze wszystkich odpowiedzi wyniosła 3,3, co można interpretować jako umiarkowanie pozytywny wynik, jednak z wyraźnie zarysowanymi różnicami między poszczególnymi segmentami rynku (wykres 14).

Najwyżej współpracę z organami ścigania ocenili reprezentanci sektora bankowego, dla którego średnia ocena wyniosła 4,0. Stosunkowo wysoko ocenili tę współpracę też respondenci z firm leasingowych (3,7). Wskazuje to, że w tych segmentach relacje z organami ścigania są zazwyczaj postrzegane jako efektywne i stabilne.

**Wykres 14.** Ocena współpracy z organami ścigania w poszczególnych branżach

Średnia z ocen w skali 1–5, gdzie „1” oznacza współpracę bardzo słabą, a „5” – bardzo dobrą

Źródło: ZPF/EY.



Nieco niższe noty pochodziły od przedstawicieli zakładów ubezpieczeń (3,0) i firm pożyczkowych (2,8), z kolei najniższą ocenę odnotowano w przypadku przedstawicieli sektora faktoringowego (2,3). Co istotne, tylko w przypadku firm faktoringowych oraz zakładów ubezpieczeń pojawiła się ocena 1, wskazująca na bardzo niskie zadowolenie ze współpracy. Może to sugerować, że zasady kontaktu z organami ścigania w pozostałych branżach objętych badaniem funkcjonują sprawniej.

W przeprowadzonych wywiadach z przedstawicielami instytucji finansowych pojawiły się dodatkowe uwagi, które uzupełniają obraz współpracy sektora finansowego z organami ścigania. Część rozmówców pozytywnie oceniła obecne relacje z przedstawicielami policji i prokuratury, podkreślając znaczący postęp w tym zakresie w porównaniu z sytuacją sprzed kilku lat. Eksperci zwracali uwagę na rozwój wspólnego języka komunikacji, większą otwartość po stronie służb oraz inicjatywy takie jak grupy robocze i konferencje, które sprzyjają budowaniu zaufania i poprawie efektywności działań. Z drugiej strony wskazywano na istotne bariery systemowe – w szczególności ograniczoną liczbę funkcjonariuszy, trudności z przetwarzaniem dużej liczby zgłoszeń oraz problemy z organizacją postępowań, które dotyczą klientów z różnych regionów Polski. Pojawiły się również głosy podkreślające specyfikę działalności niektórych segmentów rynku, takich jak leasing, gdzie działania skupiają się głównie na zapobieganiu nadużyciom, a nie na obsłudze już zaistniałych szkód. W takich przypadkach trudność stanowi m.in. brak zainteresowania organów przypadkami prób oszustw, które jeszcze nie skutkowały szkodą. W kontekście tych wyzwań eksperci postulowali rozwój systemowych rozwiązań usprawniających wymianę informacji, które mogłyby zminimalizować konieczność indywidualnych kontaktów i poprawić ciągłość operacyjną współpracy – niezależnie od rotacji personalnej po stronie służb.

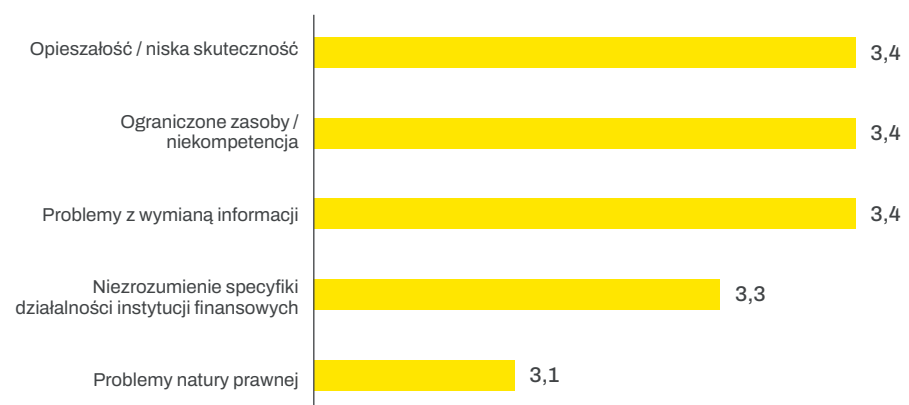
W uzupełnieniu do pytania dotyczącego ogólnej oceny współpracy z organami ścigania, respondentów poproszono o wskazanie, na ile w ich opinii istotne są konkretne problemy w tej współpracy w skali od 1 do 5 (problem mało istotny) do 5 (bardzo istotny). Pozwoliło to nie tylko określić najczęściej występujące trudności, ale również ich rzeczywiste znaczenie z perspektywy różnych typów instytucji (wykres 15).

Odpowiedzi respondentów wskazują na trzy najbardziej problematyczne kwestie: opieszałość i niską skuteczność działań organów, ograniczone zasoby lub niekompetencję funkcjonariuszy oraz problemy z wymianą informacji – wszystkie uzyskały średnią ocenę 3,4. Niższe noty otrzymały niezrozumienie specyfiki działalności instytucji finansowych (3,3) oraz problemy natury prawnej (3,1).

**Wykres 15.** Istotność problemów w relacjach z organami ścigania

Średnia z ocen w skali 1–5, gdzie „1” oznacza problem mało istotny, a „5” – bardzo istotny

Źródło: ZPF/EY.



Wyniki te wskazują, że nadal istnieje potrzeba podjęcia działań mających na celu poprawę efektywności współpracy. Wzmacnianie kompetencji funkcjonariuszy poprzez szkolenia oraz zwiększenie zasobów mogą przyczynić się do lepszego zrozumienia specyfiki sektora finansowego. Ponadto, potrzebne są usprawnienia wymiany informacji pomiędzy instytucjami finansowymi i organami ścigania. Respondenci sygnalizują, że obecne procedury wymiany danych są niewystarczające, co może

prowadzić do opóźnień w działaniach, niepełnych ustaleń operacyjnych oraz trudności w skutecznym reagowaniu na zagrożenia. Brak płynnej i efektywnej komunikacji może też wpływać na ograniczoną skuteczność w przeciwdziałaniu przestępczości gospodarczej. Również niejednoznaczność przepisów, ich rozbieżna wykładnia lub brak dostosowania do realiów operacyjnych instytucji finansowych mogą stanowić barierę utrudniającą skuteczne działanie. Wskazuje to na potrzebę dalszej harmonizacji przepisów oraz wypracowania wspólnych standardów interpretacyjnych, które zwiększyłyby przewidywalność.

W celu uzupełnienia analizy i uchwycenia potencjalnych trudności nieujętych w zamkniętym formacie kwestionariusza, respondentom umożliwiono dodatkowo swobodne wskazanie innych problemów we współpracy z organami ścigania, które ich zdaniem mają istotne znaczenie z perspektywy funkcjonowania reprezentowanej instytucji. Wśród otrzymanych odpowiedzi pojawiły się obserwacje odnoszące się do przedłużających się postępowań, braku wykonywania podstawowych czynności przez organy ścigania, niejednorodności w sposobie procedowania spraw w zależności od terytorialnej właściwości czy też zauważalnego spadku zaangażowania w prowadzenie spraw pod koniec okresów sprawozdawczych.

Przeprowadzona analiza pokazała, że współpraca z organami ścigania w ocenie instytucji finansowych obarczona jest szeregiem wyzwań, których istotność znacząco różni się w zależności od segmentu rynku. Choć żaden z problemów nie został jednoznacznie uznany za powszechny i dominujący, w wielu przypadkach uwidoczniły się trudności związane z jakością komunikacji, ograniczeniami organizacyjnymi oraz barierami prawnymi. Największe natężenie krytycznych ocen odnotowano wśród przedstawicieli firm faktoringowych i zakładów ubezpieczeń, podczas gdy instytucje bankowe częściej wskazywały na umiarkowaną lub zróżnicowaną skalę problemów. Odpowiedzi respondentów wskazują, że doświadczenia w obszarze współpracy z organami ścigania są silnie uwarunkowane specyfiką działalności i skalą operacyjną poszczególnych instytucji.



Wnioski płynące zarówno z przeprowadzonego badania ankietowego, jak i wywiadów z ekspertami potwierdzają spójność obserwacji – przedstawiciele różnych sektorów rynku finansowego wskazują na powtarzające się bariery, zagrożenia i wyzwania związane z przeciwdziałaniem nadużyciom. Przeprowadzona analiza pokazuje, że instytucje finansowe rozpoznają te same kluczowe obszary wymagające uwagi i zmian.

Pierwszym z nich jest ryzyko wynikające z dynamicznego rozwoju sztucznej inteligencji, która dzięki łatwej dostępności i niskim kosztom wdrożenia stała się narzędziem szeroko wykorzystywanym przez sprawców nadużyć. Technologia AI umożliwia generowanie fałszywych profili, dokumentów czy reklam, a także pozwala na zaawansowaną manipulację emocjami ofiar, co znacząco podnosi skuteczność przestępstw – zwłaszcza tych określanych jako tzw. friend/family fraud czy wyłudzenia inwestycyjne. Instytucje finansowe stoją w obliczu coraz bardziej złożonych oszustw, których skala i zasięg narastają wraz z rozwojem narzędzi AI, co wymaga ciągłego dostosowywania systemów ochrony i edukacji klientów.

Drugim kluczowym wątkiem jest przeregulowanie rynku, na które jednoznacznie wskazują przedstawiciele sektora. Zbyt skomplikowane, obszerne i często nieadekwatne przepisy utrudniają sprawne wdrażanie skutecznych zabezpieczeń oraz opóźniają reakcję na pojawiające się zagrożenia. Nadmiar regulacji nie dotyczy natomiast oszustów, którzy bez przeszkód wykorzystują luki i opóźnienia systemowe. Eksperti podkreślają potrzebę rozsądnej deregulacji – zwłaszcza w obszarach AML oraz wdrażania innowacji opartych na sztucznej inteligencji – by umożliwić instytucjom lepszą adaptację do zmiennych warunków rynkowych oraz skuteczną ochronę interesów klientów.

Trzeci obszar to bariery w rozwoju efektywnego przeciwdziałania nadużyciom, którymi są ograniczenia finansowe, presja na redukcję kosztów i uproszczenie procesów, a także oczekiwanie wzrostu sprzedaży i poprawy doświadczeń klienta. Wysokie koszty implementacji nowych rozwiązań i brak natychmiastowych efektów ograniczają skuteczność przeciwdziałania nadużyciom. Dodatkowo, złożone przepisy dotyczące przetwarzania danych i narzędzi AI utrudniają praktyczne wdrożenia innowacji, pomimo wysokiej motywacji i świadomości zagrożeń.

Podsumowując, należy podkreślić, że choć narzędzia i technologie są kluczowe w walce z nadużyciami, to najważniejsi pozostają ludzie – eksperci, specjaliści ds. compliance, analitycy i praktycy – których wiedza, doświadczenie oraz zaangażowanie pozwalają skutecznie identyfikować nowe zagrożenia. To właśnie ich obserwacje, spostrzeżenia i rekomendacje stanowią największą wartość dodaną zaprezentowanego raportu i wskazują kierunki dalszego rozwoju oraz koniecznych zmian w sektorze finansowym.



Związek Przedsiębiorstw Finansowych w Polsce (wcześniej Konferencja Przedsiębiorstw Finansowych w Polsce) powstał 27 października 1999 roku i obecnie skupia ponad 100 przedsiębiorstw z wielu sektorów polskiego rynku finansowego, w tym bankowości, zarządzania wierzytelnościami, pośredników finansowych, instytucji pożyczkowych, zarządzających informacją gospodarczą, odwróconej hipoteki w modelu sprzedażowym, fintech. Jest największą multisektorową organizacją podmiotów rynku finansowego w Polsce.

Od ponad 25 lat ZPF działa na rzecz rozwoju rynku finansowego w Polsce i podnoszenia standardów etycznych w branży, występuje aktywnie jako partner społeczny w procesach legislacyjnych, a także reprezentuje polskie instytucje finansowe w UE. ZPF to członek dwóch organizacji samorządowych na szczeblu europejskim: EUROFINAS (European Federation of Finance House Associations), zrzeszającej instytucje związane z rynkiem kredytu konsumenckiego w Europie oraz FENCA (Federation of European National Collection Associations), która reprezentuje interesy sektora zarządzania wierzytelnościami w Europie.

ZPF ma w swoim dorobku badawczym kilkaset raportów branżowych. Jest też organizatorem szeregu kongresów, webinarów i innych inicjatyw dla branży finansowej.



Celem działalności EY jest budowanie lepiej funkcjonującego świata poprzez wspieranie klientów, pracowników, społeczeństwa i planety w tworzeniu trwałych wartości oraz budowanie zaufania na rynkach kapitałowych.

Korzystając z danych, sztucznej inteligencji oraz zaawansowanych technologii zespoły EY pomagają klientom odważnie kształtować przyszłość i znajdować odpowiedzi na obecne i przyszłe wyzwania.

EY świadczy kompleksowe usługi w zakresie **audytu, doradztwa, podatków, strategii i transakcji**. Dzięki wiedzy sektorowej, globalnie połączonym, multidyscyplinarnym zespołom i różnorodnym partnerstwom EY może świadczyć usługi w ponad 150 krajach.

EY w Polsce to prawie 4000 specjalistów pracujących w 8 miastach: w Warszawie, Gdańsku, Katowicach, Krakowie, Łodzi, Poznaniu, Wrocławiu i Rzeszowie. Działając na polskim rynku co roku EY doradza tysiącom firm, zarówno małym i średnim przedsiębiorstwom, jak i największym korporacjom. Tworzy unikatowe analizy, dzieli się wiedzą, integruje środowisko przedsiębiorców oraz angażuje się społecznie.

Wszystko po to, aby z odwagą kształtować przyszłość.





[www.zpf.pl](http://www.zpf.pl)