

Scamy i socjotechniki w erze rozporządzenia PSR.
Jak sektor finansowy reaguje i przygotowuje się
na nadchodzące zmiany?



Maciej Jamiołkowski

Business Development Director
Fraud & Identity



06/2023

Przedstawienie projektu rozporządzenia
PSR i dyrektywy PSD3

Do końca 12/2026
Wejście PSR w życie

18 miesięcy
Na wdrożenie PSR

Najważniejsze założenia PSR pod kątem antyfraudowym w Europie



Zwiększona odpowiedzialność PSP za fraud



Monitoring transakcji w czasie rzeczywistym



Konieczność wymiany danych pomiędzy PSP



Zwrot skradzionych klientowi środków, również w związku ze scamem typu APP



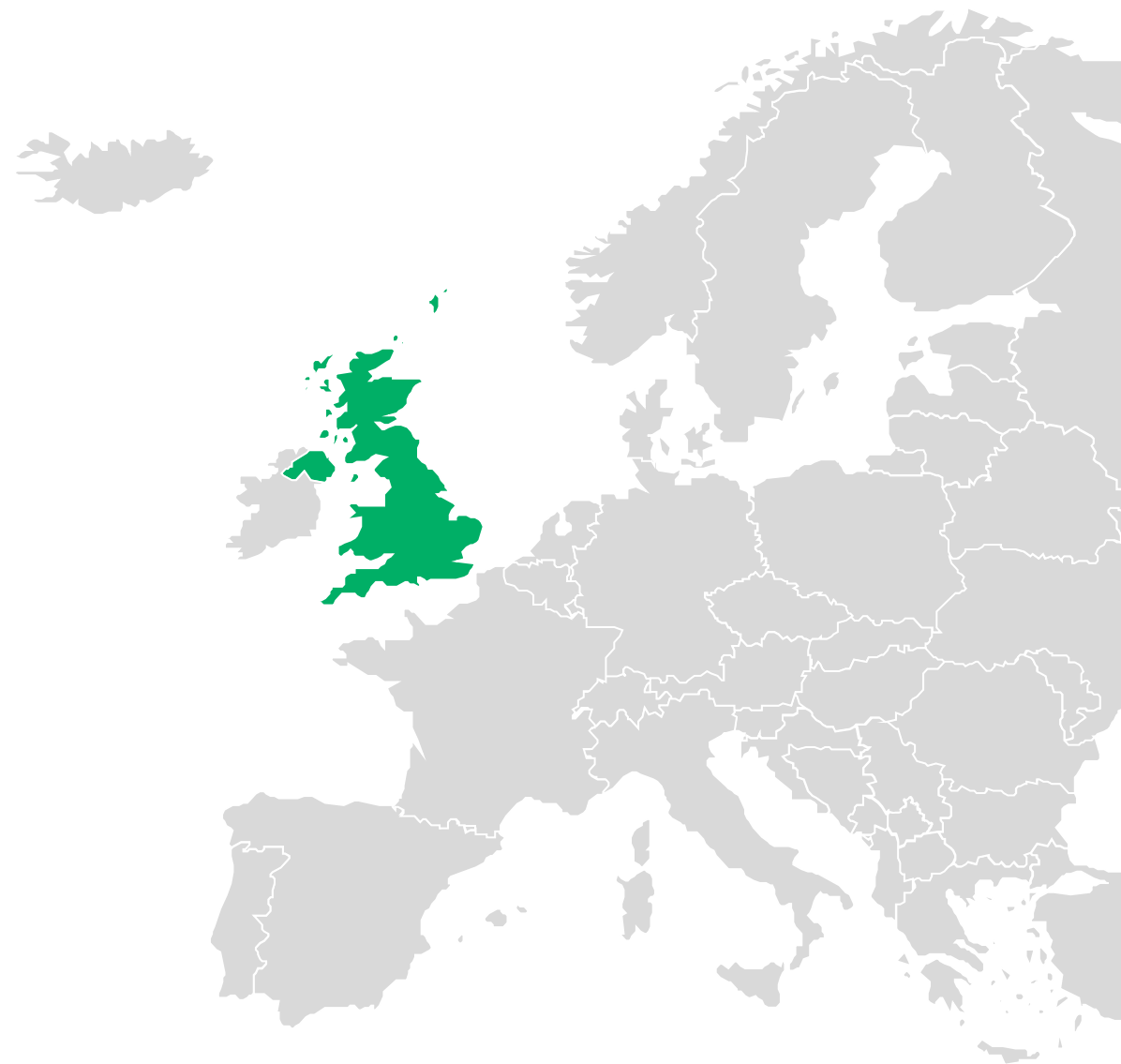
Monitorowanie przepływu środków między podmiotami



Konieczność weryfikacji odbiorcy (VoP)

Wielka Brytania

- Obowiązkowy zwrot skradzionych środków wprowadzony w 2024r. (do £85,000)
- Zwrot praktycznie pełnej kwoty skradzionych środków, w ciągu 5 dni
- Zgłoszenie w ciągu 13 miesięcy od wystąpienia zdarzenia
- **Odpowiedzialność 50/50**
(bank nadawca i bank odbiorca)



Wielka Brytania

Po roku od wprowadzenia:

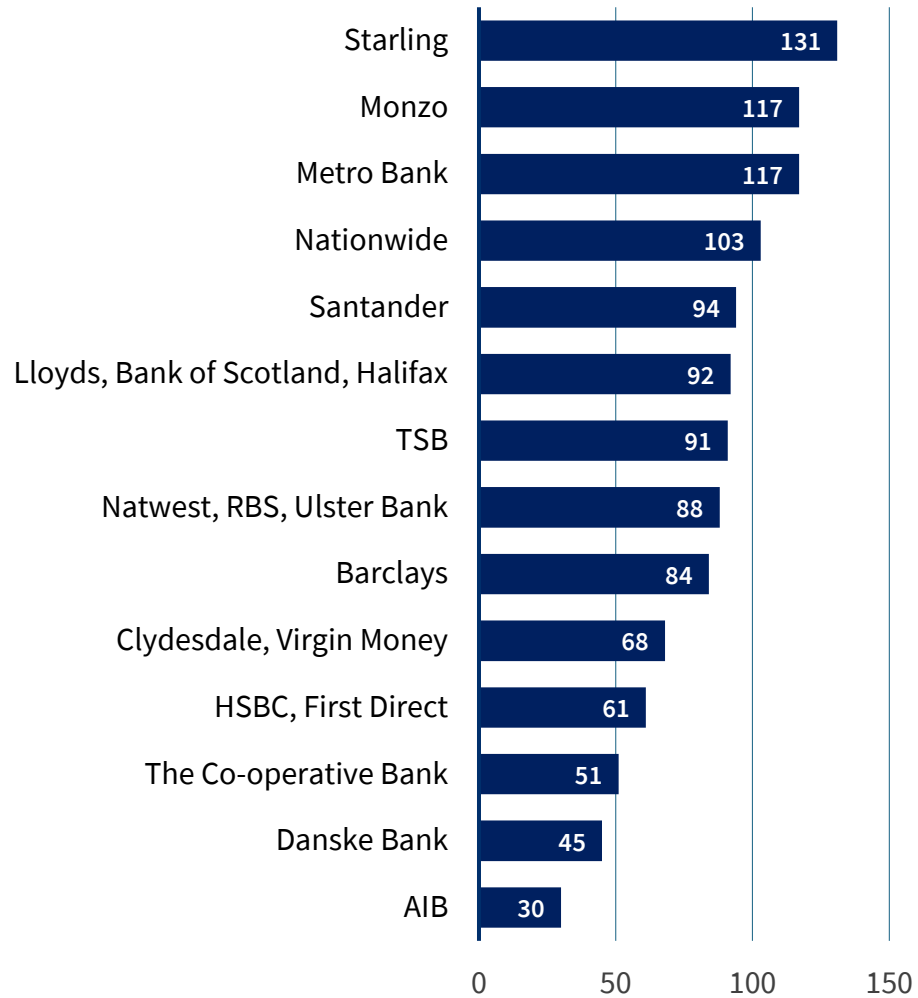
- 295 tys. zgłoszeń
- 82% zostało rozpatrzonych w ciągu 5 dni
- 88% (173 mln funtów / 850 mln zł) zwróconych środków
- 3% zgłoszeń odrzucone z powodu rażącego niedbalstwa



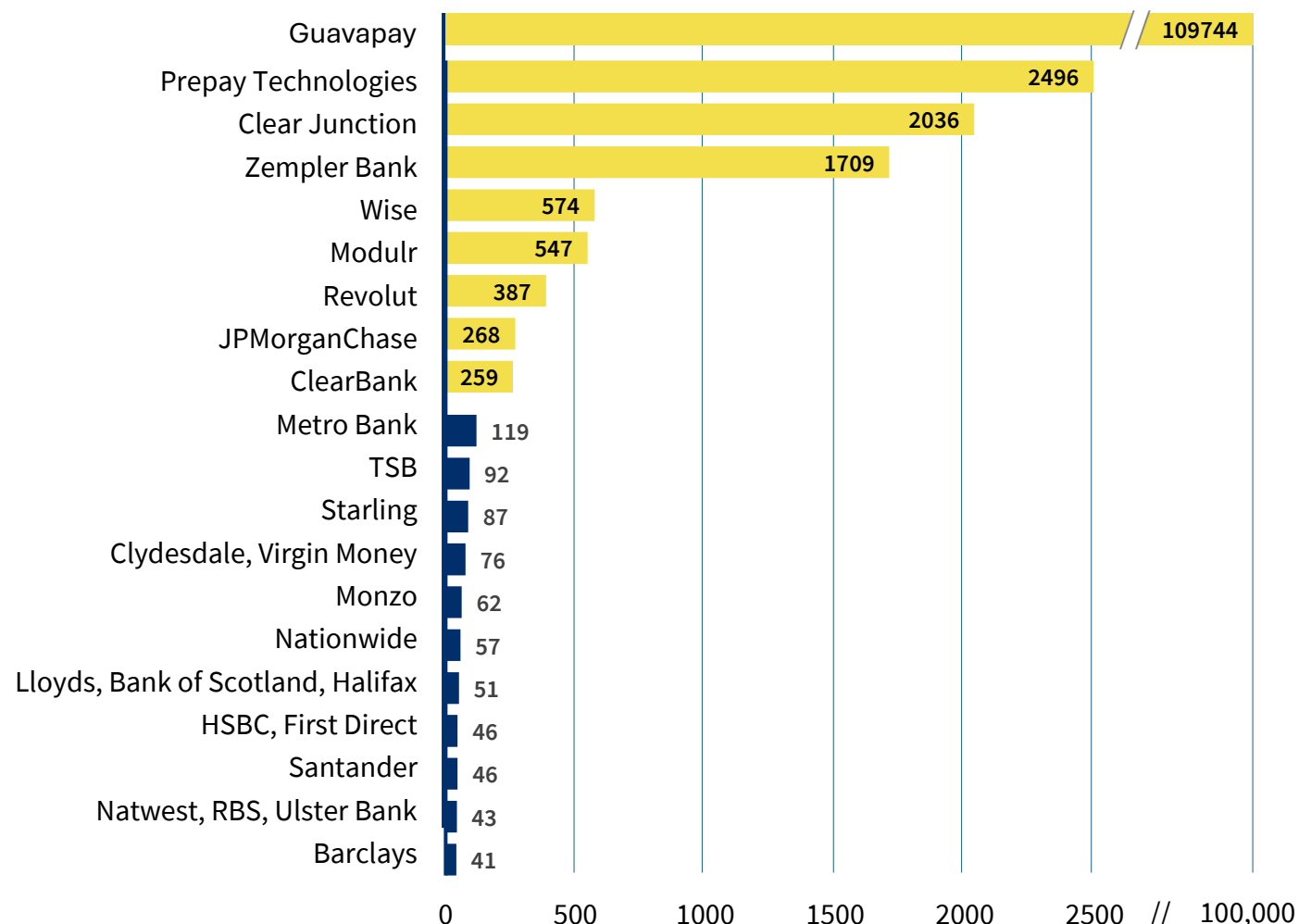
11%

redukcji scamów,
(I/II półrocze 2024 r.)

Liczba oszustw typu APP przypadająca na million transakcji



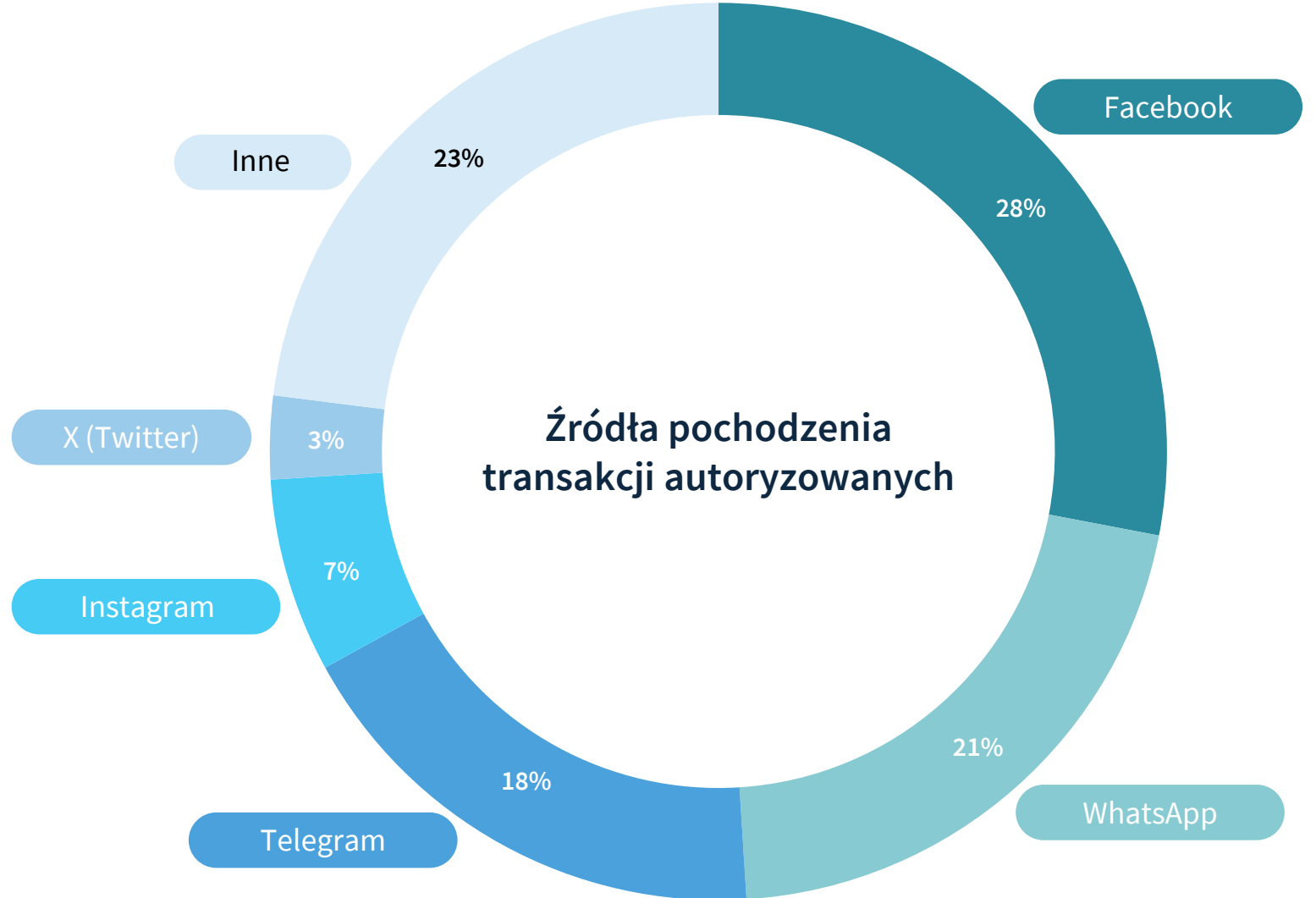
Liczba oszustw typu APP przypadająca na million transakcji



■ Non-directed (smaller) PSPs ■ Directed PSPs

Słabości PSR

20% dorosłych przyznało, że zostało oszukanych na platformach społecznościowych.

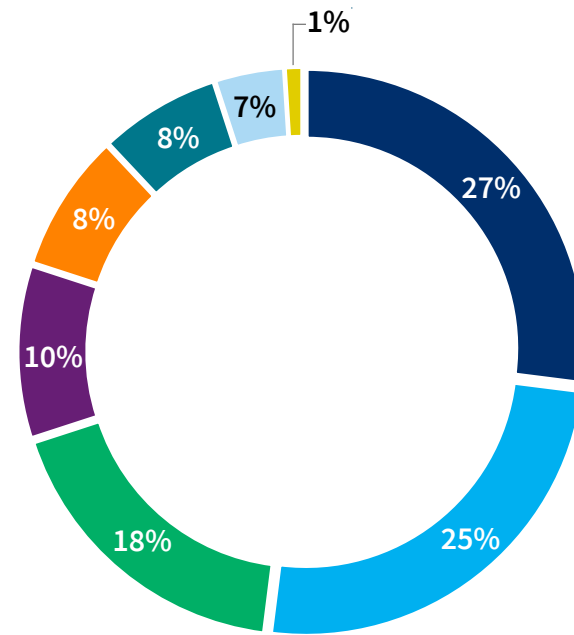


Słabości PSR

20% dorosłych przyznało, że zostało oszukanych na platformach społecznościowych.

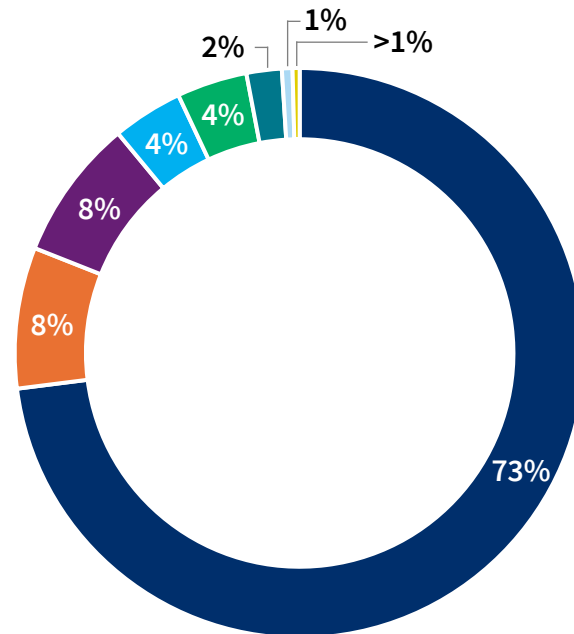
72% dorosłych zgodziło się, że banki mogłyby zrobić więcej, aby zapobiegać oszustwom.

23% dorosłych przyznało, że są mniej ostrożni od czasu wejścia w życie przepisów dotyczących zwrotów PSR.



App Scam Types by Value*

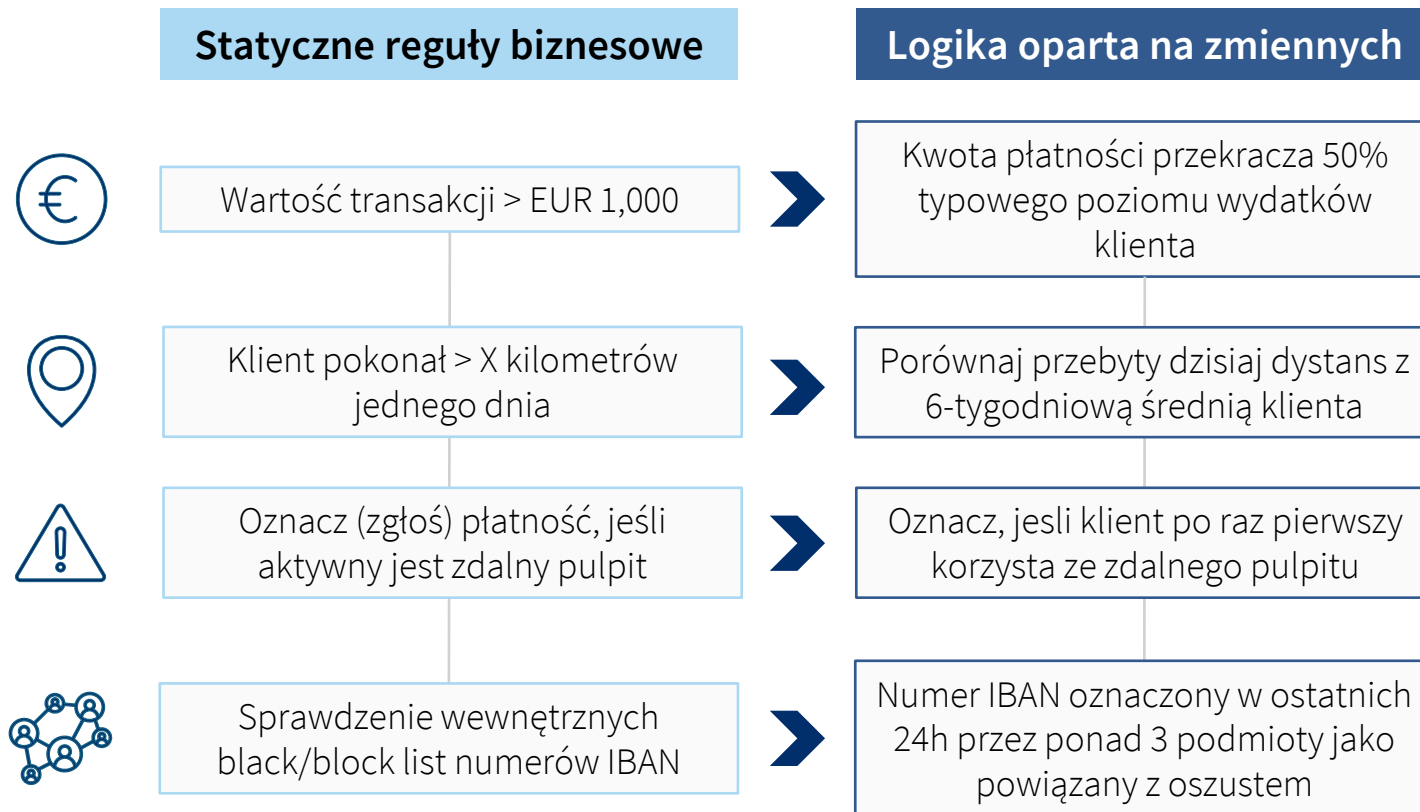
- Purchase
- Investment
- Impersonation: Police/Bank Staff
- Impersonation: Other
- Advance Fee
- Romance
- Invoice and Mandate
- Unknown Scam Type



App Scam Types by Volume*

- Purchase
- Advance Fee
- Impersonation: Other
- Investment
- Impersonation: Police/Bank Staff
- Romance
- Invoice and Mandate
- Unknown Scam Type

Mechanizmy monitoringu transakcji w myśl PSR w Wielkiej Brytanii

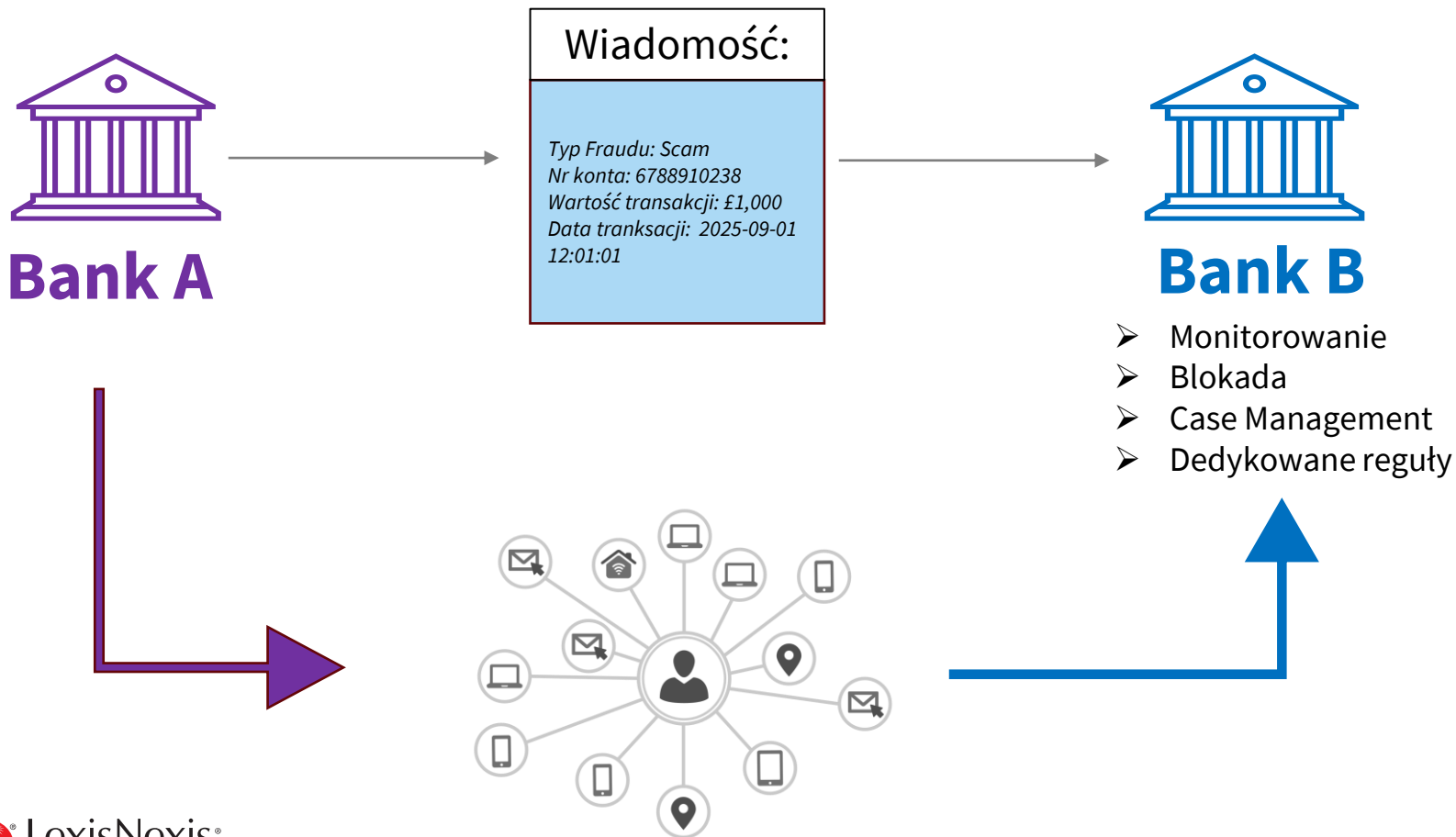


Artykuł 83 ust. 2 Mechanizmy monitorowania transakcji

Mechanizmy monitorowania transakcji powinny opierać się na analizie wcześniejszych transakcji płatniczych oraz dostępie do rachunków płatniczych online (...)

- informacje o płatniku, w tym cechy środowiskowej behawioralne typowe dla płatnika w warunkach normalnego korzystania ze spersonalizowanych danych uwierzytelniających;
- informacje o rachunku płatniczym, w tym historia transakcji płatniczych;
- informacje o transakcji, w tym kwota transakcji oraz unikalny identyfikator odbiorcy;
- dane sesji, w tym zakres adresów IP urządzenia, z którego uzyskano dostęp do rachunku płatniczego;
- (dane dotyczące urządzenia, w tym identyfikatory urządzenia.

Mechanizmy wymiany danych w myśl PSR w Wielkiej Brytanii



Artykuł 83a Wymiana danych dot. oszustw

- unikalny identyfikator odbiorcy płatności;
- nazwa odbiorcy płatności;
- unikalny identyfikator osoby fizycznej lub numer organizacyjny (firmy) odbiorcy płatności, jeżeli ma zastosowanie;
- instrument płatniczy, jeśli ma zastosowanie;
- dane transakcji, w tym kwota transakcji, waluta oraz data i godzina jej wykonania;
- dane sesji związane z potencjalnie oszukańczą transakcją, w tym zakres adresów protokołu internetowego (IP), z którego uzyskano dostęp do rachunku płatniczego;
- dane urządzenia związane z potencjalnie oszukańczą transakcją, w tym identyfikator urządzenia;
- sposób działania (modus operandi) oszustwa lub podejrzenia oszustwa;

Jak Europa przygotowuje się do PSD3/PSR?



Europa

Skandynawia, Bałtyki, Holandia i Belgia

- Najwyższa dojrzałość i gotowość regulacyjna i technologiczna
- Mocna proaktywność regulatorów
- Funkcjonująca wymiana danych pomiędzy instytucjami finansowymi
- Wysoka adaptacja Machine Learningu w detekcji fraudu real-time
- Wdrożenie zaawansowanej analizy behawioralnej

Francja i Niemcy

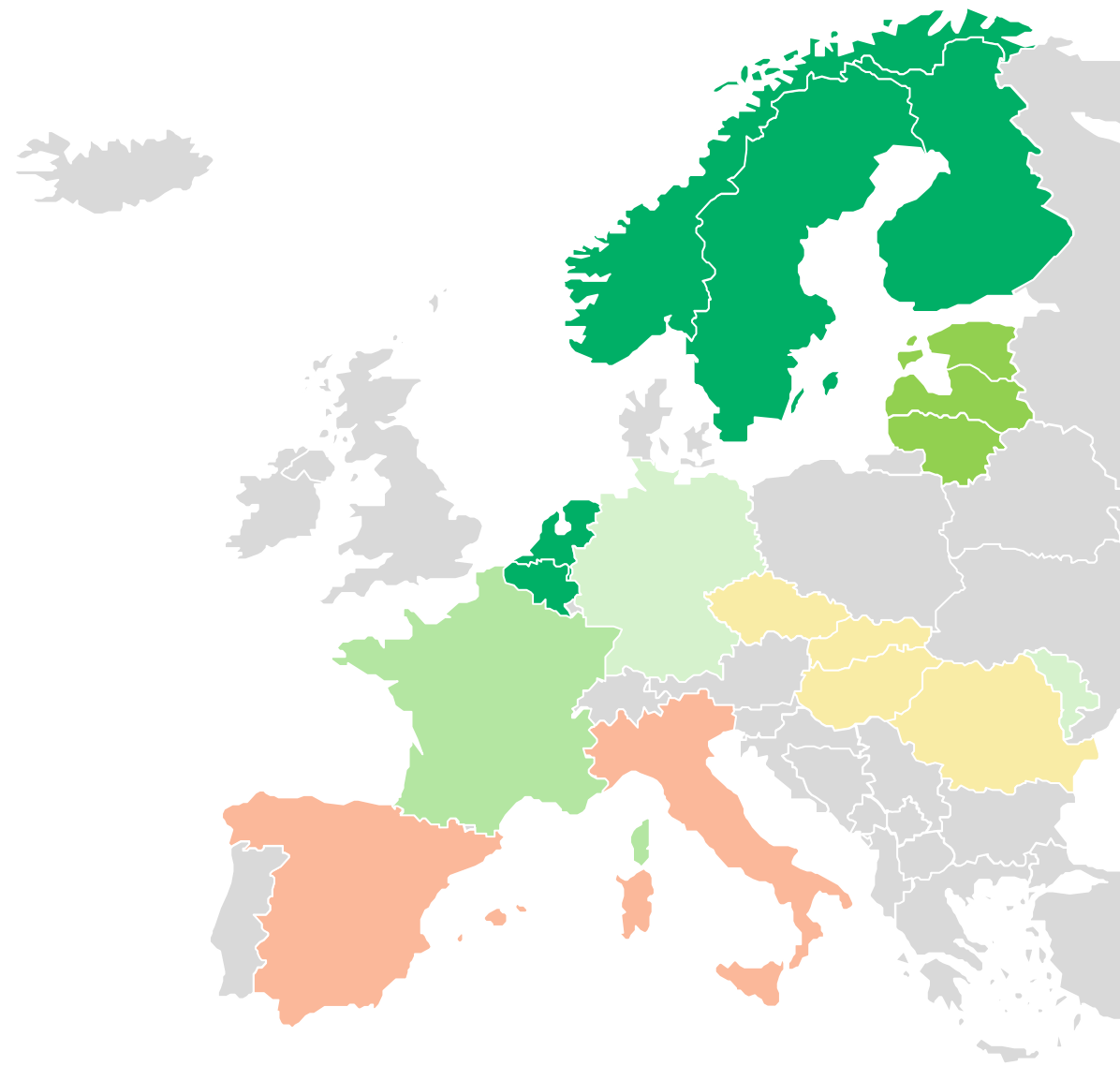
- Gotowość regulacyjna wstrzymywana przez stare i złożone systemy IT
- Duży nacisk na monitoring transakcji przychodzących
- Mocne zastosowanie Machine Learningu w detekcji fraudu transakcyjnego

Europa Centralno-Wschodnia

- Różnice implementacyjne
- Niska adopcja monitoringu transakcji w czasie rzeczywistym
- Mocno ograniczona wymiana danych między podmiotami

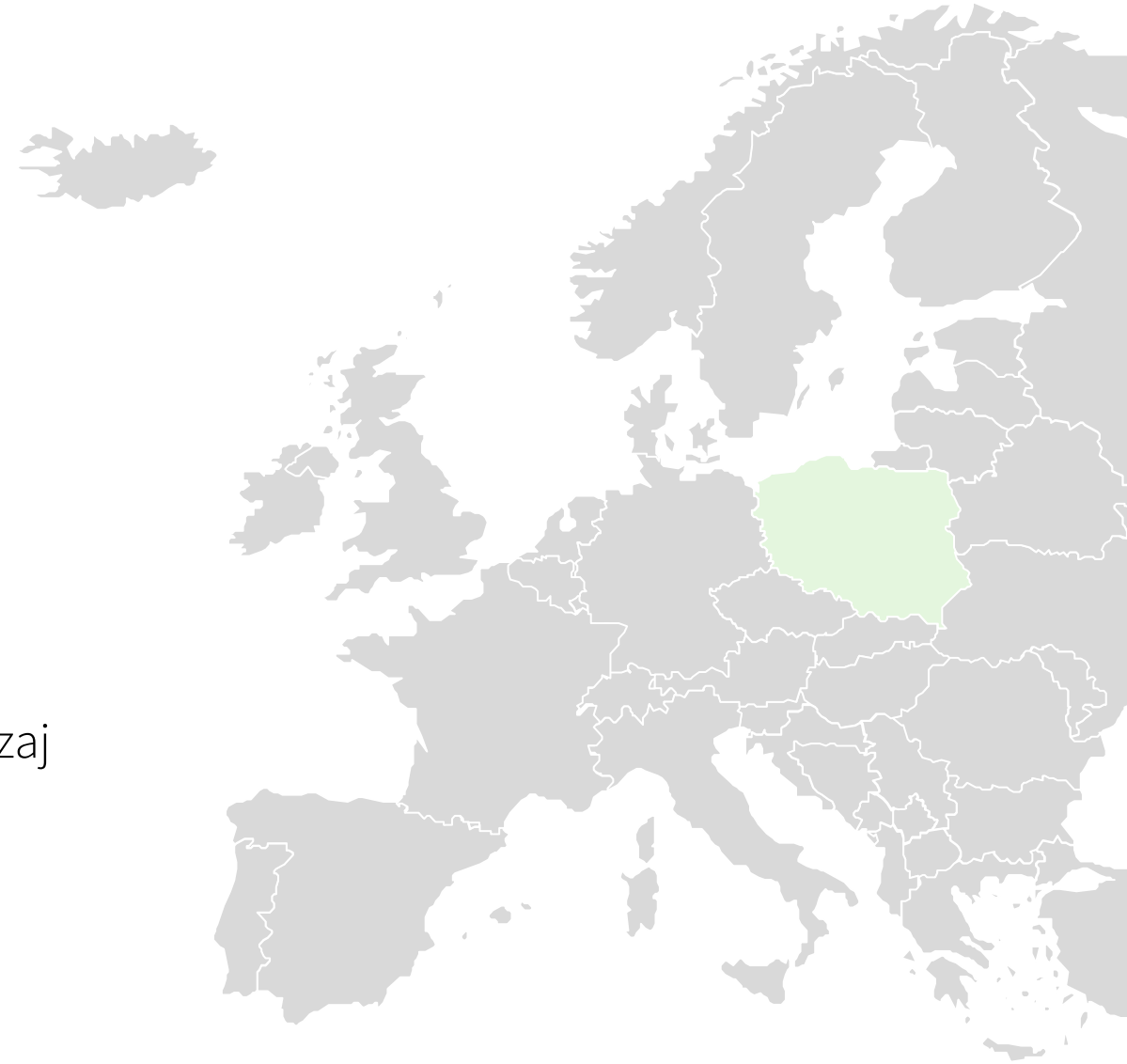
Hiszpania i Włochy

- Silnie rozdrobiony sektor bankowy
- Ograniczona skala inwestycji w zaawansowane systemy antyfraudowe



Polska

- ✓ Funkcjonujący mechanizm D+1
- ✓ Stopniowy wzrost wdrożeń monitoringu transakcji w czasie rzeczywistym
- Tajemnica bankowa i obawy przed wymianą danych
- Zbieranie zgód na analizę behawioralną
- Interpretacja dyrektyw na poziomie krajowym zazwyczaj bardziej restrykcyjna niż na poziomie ogólnounijnym



Dziękuję za uwagę!

Maciej Jamiotkowski

Business Development Director, Fraud & Identity

Zapraszam do kontaktu na LinkedIn lub mailowo:
maciej.jamiolkowski@lexisnexisrisk.com

