# Monitoring transakcji w czasie rzeczywistym

**Dariusz Wojtas**
Head of Product Management
Warszawa / 09.05.2017

# Transakcje w różnych ujęciach

- Przelewy krajowe
- Przelewy zagraniczne
- Płatności kartowe

- Natychmiastowe
- W różnych walutach
- Poprzez różne systemy pośredniczące
- Realizowane w różnych reżimach czasowych

- Przychodzące
- Wychodzące
- Raty kredytowe i leasingowe
- Weryfikacja tożsamości

- Decyzje podejmowane przez pracowników
- Przyznanie dostępu do danych
- Uruchomienie określonej akcji

# Transakcje

- Pozostawiają ślady
- Uzupełniają się
- Dotyczą zarówno klientów jak i pracowników
- Ich ilość rośnie …

- **Wg NBP** ( dane za 2016'Q4 )
  - Średnia dzienna liczba zleceń w systemie Elixir – **7,1 mln** (wzrost o **11%** w ciągu kwartału)
  - Średnia dzienna liczba zleceń w systemie EuroElixir – **0,1 mln** (wzrost o **15%** w ciągu kwartału)

  - W kwartale odnotowano **1,047 mld** transakcji przy użyciu kart płatniczych (wzrost o **3,4%** w ciągu kwartału)
  - Na koniec roku 2016 liczba terminali POS wynosiła **531 tys.** (wzrost o **3,4%** w ciągu kwartału)

# Analiza transakcji

- **Compliance**
  - Kiedyś postrzegany jako uciążliwy obowiązek
  - Dziś rośnie wewnętrzna potrzeba weryfikacji klientów i ich operacji
    - Aby zapobiec szkodzie na wizerunku
    - Aby uniknąć kar za realizację zakazanych transakcji

- **Fraudy**
  - Ochrona pieniędzy Banku i klientów przed intruzami z zewnątrz
  - Ochrona przed nieuczciwymi pracownikami

… czyli szukanie oszczędności

**Regulacyjnie rozdzielne.**

**Ale na poziomie zakresu przetwarzanych danych bardzo bliskie sobie.**

**To nie musza być rozdzielne systemy**

# Jakie to ma przełożenie na systemy?

- **Skrócenie czasu przetwarzania**

  **Batch vs Near Real time vs Real time**

- **Baza wiedzy**
  - dane z wielu źródeł w banku
  - dane z baz ogólnokrajowych (np. SWOZ, InfoDok, LOPLG, ..)
  - listy reputacyjne
  - bezpośrednia wymiana danych pomiędzy bankami

    + możliwość włączania kolejnych źródeł danych w miarę upływu czasu

- **Reguły**
  - sprawdzające określone fakty
  - sprawdzające złożone relacje pomiędzy danymi z różnych źródeł
  - pozwalające na liczenie ryzyk zależnych od kontekstu

- **Raportowanie i statystyki**

# Źródła danych

**Dotychczasowe / tradycyjne**

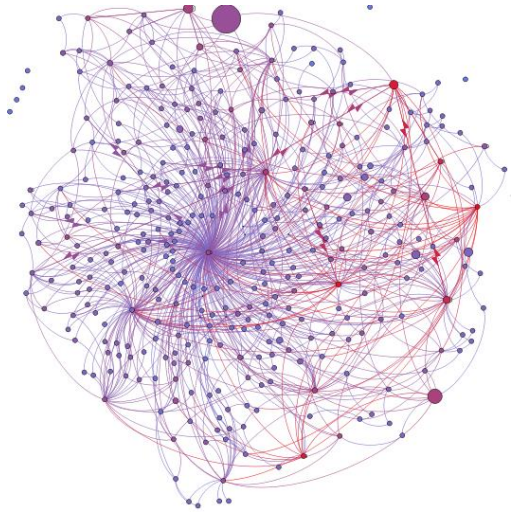
- System core'owy
- Bankowość elektroniczna
- Bankowość mobilna
- Systemy kredytowe
- Logi opisujące działania pracowników
- Informacje z systemów HR banku

- Bazy ogólnokrajowe
- Bazy międzynarodowe

**Nowe**

- Bezpośredni monitoring kanału webowego
- Dane z mediów społecznościowych
- Bazy wiarygodności urządzeń
- Centralny Rejestr Beneficjentów Rzeczywistych

- Bezpośrednia wymiana danych pomiędzy bankami



# Przykłady – skąd biorą się reguły i know-how?

- 15-go maja 2016 **w Japonii** wyprowadzono przez wypłaty z bankomatów około 13 mln $
  - ponad 100 oszustów
  - 1 700 bankomatów
  - krótki czas – pomiędzy 5 a 8 rano
  - maksymalne dopuszczalne wypłaty – 100 000 jenów (~913 $)
  - duplikaty kart kredytowych stworzonych na bazie danych skradzionych z South Africa's Standard Bank

- W 2015 **w Polsce** miały miejsce kradzieże z kont klientów banków za sprawą innowacyjnej usługi SMS
  - Jeden z operatorów komórkowych wprowadził usługę wysyłania duplikatu SMS na komputer
  - Złodzieje skanowali przejęte konta emailowe pod kątem posiadania faktur od tego operatora
  - Wytypowanych klientów operatora atakowali spamem, który miał zainfekować ich komputery
    - Podsłuchiwanie loginów i haseł do serwisu operatora komórkowego
    - Podsłuchiwanie loginów i haseł do bankowości elektronicznej
  - Wykorzystanie tych danych do przekierowania SMSów na własne komputery
  - Kradzież z rachunków klientów
    - Zrywanie lokat, przelewanie środków na konta słupów, szybkie wypłaty w bankomatach
    - Aby obejść limity dzienne wypłat – operacje tuż przed i tuż po północy

# Przykłady – skąd biorą się reguły i know-how?

- W 2017 **w Niemczech** odnotowano przypadki przekierowywania SMSów z kodami jednorazowymi na telefony złodziejów. Wymagało to
  - znajomości protokołu SS7 (protokół telekomunikacyjny)
  - dostępu do infrastruktury operatora telekomunikacyjnego (podobno wydatek rzędu 1 000 EUR)
  - znalezienie takiego operatora telco, który nie filtruje restrykcyjnie ruchu z sieci innych operatorów
  - wytypowania/znalezienia klientów banków, którzy mieli komórki w sieci tego operatora
  - infekcji maszyn tych klientów
  - podsłuchania loginów i haseł do kont bankowych i wykradzenie numerów telefonów do potwierdzeń
  - przekierowanie SMSów wysyłanych do klientów na swoje telefony

- Banki wymieniają się informacjami o **słupach / mułach**
  - Otwarcie rachunku przez taką osobę może mieć na celu dokonanie przestępstwa
  - Podobnie sprawdzeniu podlega to czy klient nie jest obywatelem państwa, z którego klienci podlegają specjalnemu monitoringowi

  - Operacje na rachunkach takich klientów powinny podlegać dodatkowemu monitoringowi, szczególnie wpływy na rachunek na kwotę powyżej określonego progu progu

# Przykłady – skąd biorą się reguły i know-how?

- Zdarza się, że transakcje zlecane z adresów IP znajdujących się na monitorowanych listach
  - Czarne listy, np. **Lista węzłów Tor**
    - Można je regularnie aktualizować, w cyklach nawet co kilkadziesiąt minut
    - … ale czy klient nie należy do tych, którzy świadomie tak działają z własnym bankiem? Na whitelistę go?
  - **Zagraniczne numery IP**, czasem te same dla większej ilości klientów
    - Może to być spowodowane tym, że ktoś pracuje w korporacji, która ma określone wyjścia na świat z sieci firmowej
    - Zidentyfikowany numer IP na dedykowaną whitelistę?

# Co jest ważne aby efektywnie walczyć z takimi oszustwami?

- Śledzić nietypowe zachowania:
  - Masowe zdarzenia
  - Analizować doniesienia o oszustwach w banku
  - Analizować alerty o sytuacjach nietypowych dla profilu zachowań klienta

- Móc szybko zareagować i przelać tę wiedzę do systemu antyfraudowego
  - Wykorzystanie wszystkich dostępnych informacji niesionych przez transakcje
  - Obsługa patternów

- Jeśli to potrzebne, zasilać **Bazę wiedzy** kolejnymi danymi i określić zależności pomiędzy tymi danymi

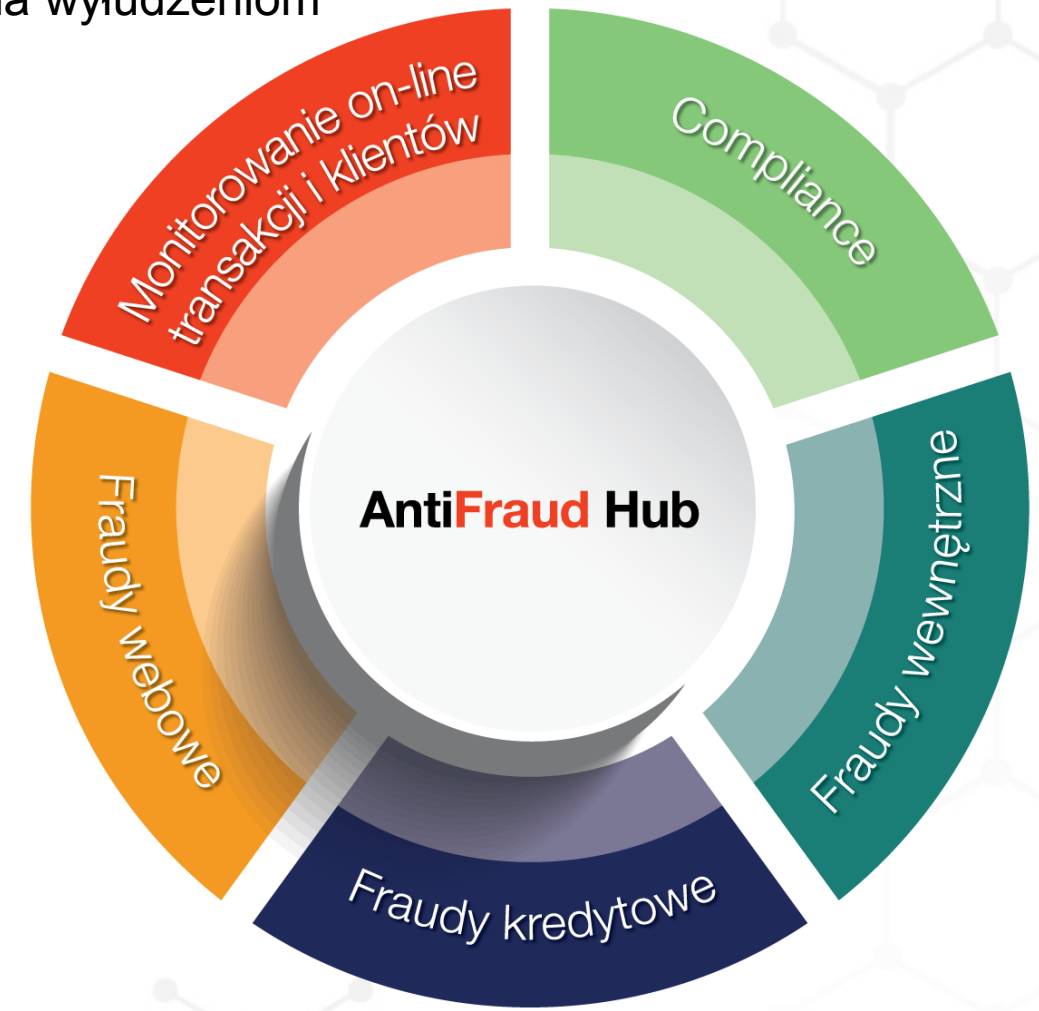
**Być na bieżąco z wiedzą z branży i umieć opisać scenariusze wyłudzeń.**

# Korzyści

- Uniknięcie lub redukcja strat finansowych
  - Wyprowadzanie pieniędzy klientów
  - Ograniczanie ilości wyłudzeń kredytowych
- Zapobieganie szkodom reputacyjnym
- Redukcja ryzyka związanego z obszarem compliance
- Ściślejszy monitoring pracowników w sektorze odznaczającym się wysoką rotacją

# IMPAQ AntiFraud Hub

- **AntiFraud Hub** to nowoczesna platforma do zapobiegania wyłudzeniom
  - Współpracuje z naszym rozwiązaniem **kdprevent**, które pokrywa obszary Compliance
- **AntiFraud Hub** obejmuje różne obszary biznesowe
  - Compliance
  - Fraudy Wewnętrzne
  - Monitorowanie aplikacji kredytowych i leasingowych
  - Fraudy webowe
  - Monitorowanie transakcji w czasie rzeczywistym
- **AntiFraud Hub** jest aktywnie rozwijany i kolejne obszary do monitorowania to
  - Płatności elektroniczne
  - Obsługa szkód w ubezpieczeniach
  - Wiarygodność urządzeń
  - E-Commerce



# IMPAQ AntiFraud Hub

- Online'owe działanie
- Skalowalność
- Automatyczne podejmowanie decyzji
- Pełna audytowalność
- Baza wiedzy obejmująca dane z różnych źródeł
- Connectory do różnych źródeł zewnętrznych
- Obsługa Beneficjentów rzeczywistych
- Baza Incydentów
- Obsługa spraw
- Rejestr pism i wsparcie dla korespondencji z organami