Jakość, kompletność i standaryzacja danych – czynniki wpływające na przeciwdziałanie oszustwom finansowym

Kluczowym elementem w procesie przeciwdziałania nadużyciom jest wymiana informacji o stwierdzonych fraudach między instytucjami finansowymi. W wykrywalności przestępstw istotne jest przekazywanie dobrego jakościowo i szerokiego zakresu informacji towarzyszących bądź wykorzystanych w wyłudzeniu lub próbie wyłudzenia. Przestępcy bowiem, w przypadku skutecznego ataku na jedną instytucję, zazwyczaj powielają schemat swojego działania, a niejednokrotnie także dane użyte do konkretnego wyłudzenia wykorzystywane są w kolejnych instytucjach. U podstaw skutecznego wykrywania tego typu przestępstw leży automatyzacja procesu, jego kompleksowość, a w tym standaryzacja danych.

Bartosz Wójcicki
Departament Produktów Bankowych BIK S.A.

Czym jest fraud – definicje

Aby skutecznie przeciwdziałać stratom instytucji finansowych z tytułu nadużyć (popularnie nazywanymi „fraudami"), należy w pierwszej kolejności zastanowić się nad definicją, czyli odpowiedzieć sobie na pytanie, czym tak naprawdę jest fraud. W *Kodeksie karnym* zostały określone przepisy obejmujące swoim zakresem zarówno oszustwo (art. 286 k.k.), jak również oszustwo kredytowe (art. 297 k.k.), jednak wydaje się, że nie wyczerpują one wszystkich możliwych przypadków wystąpienia fraudu. W ocenie praktyków jedną z najtrafniejszych definicji fraudu jest ta opracowana przy współpracy stowarzyszeń Biegłych ds. Wykrywania Nadużyć Gospodarczych (ACFE), Audytorów Wewnętrznych (IIA) oraz Amerykańskiego Instytutu Biegłych Rewidentów (AICPA). Zgodnie z tą definicją nadużycie gospodarcze jest to każde celowe działanie bądź zaniedbanie skutkujące osiągnięciem korzyści przez sprawcę lub poniesieniem straty przez ofiarę, dokonane za pomocą wprowadzenia w błąd. Ta definicja pośrednio wskazuje także na podstawową różnicę pomiędzy ryzykiem kredytowym a ryzykiem wyłudzenia (które jest elementem ryzyka operacyjnego) – w przypadku ryzyka kredytowego klient ma intencję spłaty. Z kolei w przypadku wyłudzeń mamy do czynienia z brakiem takiej intencji już od początku ubiegania się przez potencjalnego klienta o finansowanie. O ile wspólnym punktem na właściwą ocenę zarówno ryzyka kredytowego, jak i operacyjnego jest moment analizy aplikacji kredytowej (wniosku o kredyt), to największą trudnością w wychwytywaniu nadużyć jest właśnie uchwycenie faktu celowego działania przestępcy. W celu zwiększenia skuteczności wychwytywania aplikacji kredytowych charakteryzujących się zwiększonym ryzykiem wyłudzenia instytucje finansowe korzystają z zaawansowanych rozwiązań informatycznych, które wspierają proces detekcji takich aplikacji kredytowych.

Standaryzacja danych

Systemy antyfraudowe działają na zasadzie porównywania danych z bieżącej aplikacji kredytowej z innymi aplikacjami (także historycznymi). W przypadku korelacji danych (lub nieścisłości w podawanych w danej aplikacji kredytowej informacji) systemy te oznaczają dany wniosek jako wymagający dodatkowej analizy. Oczywisty jest fakt, że dane użyte do takiego porównania powinny być jak najlepszej jakości, w szczególności muszą być wystandaryzowane. Bo o ile standaryzacja danych, np. teleadresowych, dla potrzeb oceny ryzyka kredytowego jest sprawą mniej istotną, to w przypadku weryfikacji antyfraudowej może mieć kluczowe znaczenie. Aspekt ten można wyjaśnić na prostym przykładzie adresu: na potrzeby dostarczenia korespondencji nie ma znaczenia, czy w systemie informatycznym ulica będzie figurowała jako „Myszkowa 1 m. 3" czy też „Myszkowa 1 lok. 3". Bez standaryzacji danych system potraktuje powyższe zapisy jako dwa różne adresy. Ponadto standaryzacja danych pozwala na wyeliminowanie typowo „pisarskich" błędów („Myzskowa"), czy też, korelując dane z danymi z baz adresowych, pozwala wychwycić przypadki nieistniejących ulic. W rzeczywistości zależności w danych, na których opiera się działanie systemu antyfraudowego, jest znacząco więcej: dochód netto/brutto, numer telefonu („+48 12345678" / „123456789" itp.). Normalizacja informacji na wejściu musi przede wszystkim zapewnić zmniejszenie ilości błędnie powiązanych danych oraz zapewnić powiązywanie danych, które omyłkowo zostały pominięte. Wszystko po to, aby nie generować fałszywych alertów („*false positive*") wymagających pracy analityków odpowiedzialnych w instytucji finansowej za analizę antyfraudową.

Jakość danych

Jakość informacji nie odnosi się tylko do danych wprowadzanych do systemów informatycznych poszczególnych instytucji finansowych. Jakość to cały proces zbierania danych, w którym istotne znacznie mają dane pozyskiwane od potencjalnych klientów. Jednym z przykładów nadużyć są przypadki potocznie nazywane **1st Party Fraud**. W takich przypadkach wnioskodawca kreuje fałszywą rzeczywistość, „podkolorowując" swoją sytuację (zawyżanie dochodów, zaniża-

nie wydatków itp.) w celu uzyskania kredytu czy pożyczki w kwocie przewyższającej posiadaną przez niego zdolność do terminowego regulowania zobowiązań. Często może to nie być świadoma chęć wyłudzania, ale pragnienie dokonania zakupu wymarzonego domu, samochodu lub sfinansowania potrzeby prowadzonego przedsiębiorstwa. Osoby te często nie zdają sobie sprawy, że podanie prawdziwych i rzetelnych danych leży przede wszystkim w ich własnym interesie. Prawidłowa ocena zdolności kredytowej ma chronić nie tylko bank przed brakiem możliwości odzyskania długu, ale przede wszystkim kredytobiorców przez przekredytowaniem – czyli sytuacją, w której nie są w stanie spłacić swoich zobowiązań. Ponadto, upraszczając, instytucjom finansowym nie zależy na udzielaniu „złych" kredytów i ponoszeniu dodatkowych kosztów związanych z ich obsługą (np. windykacja).

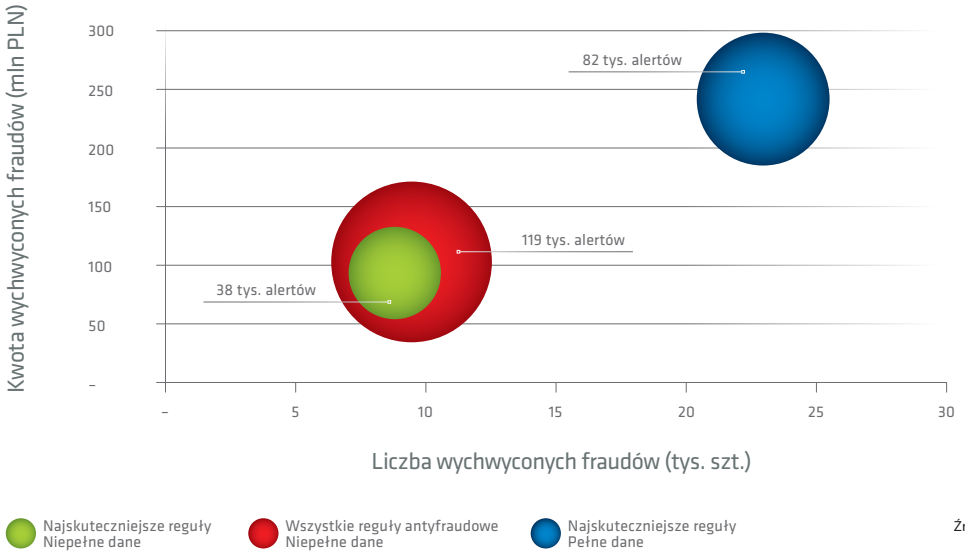
Kompletność danych

Oczywiście nieco inna sytuacja jest w przypadku przestępców, którzy świadomie podają nieprawdziwe dane (w szczególności dane ze skradzionych tożsamości) – nadużycia tego typu nazywane są często **3rd Party Fraud**. W takich przypadkach wykrywane są najczęściej niekonsekwencje (np. rozbieżności danych o osobach na utrzymaniu czy miesięcznych wydatkach itp.), które podczas analizy antyfraudowej wskazują właśnie na próbę nadużycia. Tak więc kompletność przetwarzanych danych w systemach informatycznych ma także istotne znacznie na wykrywanie prób nadużyć. Ponadto działania wychwytujące niekonsekwencje lub rozbieżności w podawanych danych również mają na celu ochronę rzeczywistych osób, którym np. skradziono dokument tożsamości lub ich dane dostały się w niepowołane ręce.

Zakres przetwarzanych danych – wymiar sektorowy

Systemem umożliwiającym wymianę danych między uczestnikami rynku kredytowego w Polsce jest Platforma Antyfraudowa BIK – narzędzie automatyzujące proces wymiany informacji, w szczególności uwzględniające przypadki zakwalifikowane jako wyłudzenia, w stosunku do których nastąpiło zgłoszenie do organów ścigania. I w przypadku tego systemu jakość i zakres danych ma olbrzymie znaczenie. Przygotowując się do wdrożenia tego typu rozwiązania, BIK przeprowadził symulację skuteczności Platformy Antyfraudowej w przypadku wdrożenia jej w całym sektorze bankowym. Jej wyniki jednoznacznie wskazują, że bardzo ważnym elementem pozwalającym na zwiększenie wykrywalności przestępstw jest przekazywanie dobrego jakościowo, szerokiego zakresu informacji towarzyszących bądź wykorzystanych w wyłudzeniu lub próbie wyłudzenia. Zależność tę prezentuje 1.

1. Zakres danych a wykrywalność fraudów



Źródło: BIK S.A.

Ze wspominanego badania wynika, iż budowanie nawet bardzo wysublimowanych reguł antyfraudowych, jednak bazujących na niepełnych danych, zwiększa znacząco liczbę generowanych przez platformę alertów, przy nieznacznym tylko zwiększeniu ilości i kwoty wykrytych przypadków. Jednak zwiększenie zakresu danych (oczywiście dobrej jakości) już przy zastosowaniu podstawowego zestawu reguł antyfraudowych znacząco zwiększa wykrywalność.

Platforma Antyfraudowa – kompleksowe rozwiązanie dla sektora finansowego

Wdrożona przez Biuro Informacji Kredytowej Platforma Antyfraudowa jest rozwiązaniem kompleksowym. Z jednej strony stanowi kompletny system antyfraudowy dedykowany do procesów kredytowych, umożliwiający elastyczne zarządzanie zarówno zakresem danych, jak i regułami bazującymi na tych danych. Z drugiej strony – rozwiązanie to pozwala na wymianę danych o zidentyfikowanych przypadkach nadużyć w sektorze. Należy jednakże podkreślić, że Platforma Antyfraudowa nie jest w stanie samodzielnie „stwierdzić", czy w danym przypadku doszło do wyłudzenia, czy jest to tylko przypadkowa zbieżność danych. Zadanie weryfikacji wskazań Platformy Antyfraudowej wykonuje analityk antyfraudowy po stronie instytucji, która otrzymała „alert" z Platformy. Dopiero w wyniku takiej weryfikacji (kompleksowej analizy antyfraudowej) możliwe jest wskazanie, czy doszło do popełnienia przestępstwa (próby wyłudzenia). Projektując Platformę Antyfraudową, BIK wziął pod uwagę oczekiwania sektora bankowego, ale także najlepsze praktyki z rynków finansowych innych krajów. Tego typu rozwiązania są sprawdzonymi mechanizmami w walce z oszustwami finansowymi i przynoszą realne oszczędności, nie dopuszczając do uruchomienia kredytów, w przypadku których może dojść do wyłudzenia. Ponadto dla uczestników Platformy Antyfraudowej, którzy przestąpią do systemu w tym roku, Biuro Informacji Kredytowej przygotowało specjalne oferty promocyjne. ■