

Tylko ścisła współpraca banków w zakresie przeciwdziałania wyłudzeniom – kluczem ograniczania strat fraudowych

Ta prosta prawda tylko z pozoru wydaje się oczywista, bowiem wiedza na temat skali i zasięgu zjawiska wyłudzeń, pomimo upływu lat, pozostaje zróżnicowana, a ponadto świadomość, że razem możemy więcej, nie jest do końca powszechna. Również dlatego, przekonując do współpracy kolejne instytucje finansowe, wciąż musimy doskonalić dostępne instrumenty i narzędzia wymiany informacji. Sprawą o podstawowym znaczeniu jest możliwość szybkiego rozpoznawania potencjalnych zagrożeń w odniesieniu do poszczególnych transakcji kredytowych.

Witold Krajewski, Departament Rynku Bankowego BIK S.A.

Trudno jest pozyskać informacje o rzeczywistej skali wyłudzeń kredytów w polskim sektorze bankowym. Wynika to z wielu przyczyn, takich jak np. brak rzetelnej weryfikacji fraudowej, ograniczeń kadrowych w bankach, rejestracji wyłudzeń jako straty kredytowe.

Analiza na podstawie danych BIK z lat 2011–2013 wykazała możliwą skalę problemu wyłudzeń w bankach na poziomie ok. 0,4–0,45 proc. kwoty udzielanych kredytów, co stanowi wartość 450–500 mln zł rocznie.

Jako założenia do identyfikacji transakcji wyłudzonych przyjęto warunki:

- rachunki kredytowe, gdzie brak spłaty pierwszej raty,
- rachunki kredytowe, gdzie całkowicie ustaje ich obsługa w przeciągu pierwszych sześciu miesięcy od udzielenia kredytu,
- rachunki kredytowe z trzema brakującymi płatnościami w przeciągu pierwszych sześciu miesięcy od udzielenia kredytu.

Liczba i wartość transakcji wyłudzonych zrodziła wśród banków potrzebę stworzenia platformy do wymiany informacji, w ramach której będą one mogły wymieniać się danymi, zakwali-

fikowanymi jako potencjalne obciążone ryzykiem fraudowym bądź niosące podwyższone ryzyko nadużyć.

Założenia i podstawy formalnoprawne budowy BLOW

BIK wspólnie z bankami zbudował System antyfraudowy Baza Informacji – Weryfikacja (BLOW), który umożliwia realizowanie potrzeby wzajemnej wymiany danych pomiędzy bankami w celu przeciwdziałania wyłudzeniom.

W BLOW są przetwarzane w szczególności dane stanowiące tajemnicę bankową oraz dane, których rodzaj i użyteczność wskazują na potrzebę ich wymiany w sektorze bankowym.

Baza Systemu antyfraudowego BLOW, z uwagi na przetwarzanie danych wrażliwych, jest zarejestrowana w GODO. Podstawą prawną do przetwarzania danych w tym Systemie jest art. 106 litera d ustawy *Prawo bankowe*. System BLOW spełnia wymagania wynikające

z *Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*.

W BLOW są przetwarzane w szczególności dane stanowiące tajemnicę bankową oraz dane, których rodzaj i użyteczność wskazują na potrzebę ich wymiany w sektorze bankowym. Decyzja o umieszczeniu danych w bazie jest suwerenną i autonomiczną decyzją banku wprowadzającego dane. W systemie dostępne są informacje dotyczące danych podmiotów gospodarczych oraz osób fizycznych.

Zakres przetwarzanych danych obejmuje w szczególności:

- Dane **identyfikacyjne** (PESEL, NIP, REGON)
- Dane **dokumentów tożsamości**
- Dane dotyczące **telefonów**
- Dane dotyczące **adresów zamieszkania i zameldowania**
- Dane dotyczące **adresów e-mail, numerów rachunków bankowych**
- Dane dotyczące **rodzaju ryzyka danych (kategoria)**
- Dane dotyczące **zgłoszenia do organu ścigania**

Bank wprowadzający dane pozostaje ich właścicielem w Systemie BIOR i tylko on może je modyfikować. Wprowadzone zasoby informacyjne poprzez przypisaną kategorię wskazują na poziom związanego z nimi ryzyka. Aktualnie stosowana typologia definiuje 8 kategorii dla danych podmiotów gospodarczych oraz 8 dla danych osób fizycznych. System BIOR pozostaje otwarty, co umożliwia definiowanie nowych kategorii, zgodnie z oczekiwaniami i potrzebami jego użytkowników.

Wprowadzone do BIOR dane osobowe, w przypadku ustania możliwości ich przetwarzania, są usuwane poprzez ich anonimizację, co wynika z wymogów *Ustawy o ochronie danych osobowych*.

W celu zapewnienia sprawnego i efektywnego procesu wyjaśniania powodów wprowadzenia danych System BIOR umożliwia identyfikację banku, który wprowadził dane, wspierając również komunikację drogą elektroniczną (e-mail).

Szczególną uwagę w ramach Systemu BIOR należy zwrócić na dane przetwarzane w ramach kategorii *Rachunek skompromitowany*. Jest to kategoria wprowadzona po zidentyfikowaniu w sektorze bankowym przypadków zakładania rachunków bankowych na fałszywe lub ukradzione dane osobowe, które to rachunki następnie były wykorzystywane w celach przestępczych. Możliwość wymiany informacji o takich rachunkach pomaga ograniczać wyłudzenia środków finansowych, jak również pozwala przeciwdziałać praniu pieniędzy.

Dostęp i sposoby wykorzystania danych z Systemu BIOR

W ramach Systemu BIOR są zdefiniowane trzy poziomy (role), określające zakres dostępu, dla operacyjnego korzystania z systemu:

- Rola *Analitik* umożliwiająca wprowadzanie, aktualizowanie i usuwanie danych, wyszukiwanie danych po szeroko zdefiniowanych parametrach wyszukiwania oraz generowanie raportów danych. Osoby posiadające tę przypisaną rolę są właścicielami danych w BIOR.
- Rola *Referent* umożliwiająca wyszukiwanie danych po szeroko definiowa-

nych parametrach wyszukiwania oraz generowanie raportów danych.

- Rola *Koordinator* umożliwiająca generowanie raportów aktywności użytkowników w BIOR oraz przypisywanie danych do *Analitików*.

Bazowym kanałem dostępu do BIOR jest strona WWW, w ramach której możliwe są wszystkie operacje wykonywane na danych w BIOR, takie jak: wprowadzanie, aktualizowanie, usuwanie, wyszukiwanie, generowanie raportów oraz generowanie zapytań do banków dotyczących wprowadzonych danych.

Kolejnym kanałem dostępowym w zakresie odpytywania automatycznego Systemu BIOR jest możliwość pozyskiwania alertów z BIOR w raportach kredytowych BIK. Bank, składając zapytanie w ramach Systemu Informacyjnego BIK Klient Indywidualny (wersja 3.7), może otrzymać informację o wyniku przeszukania Systemu BIOR w odniesieniu do danych wskazanych w zapytaniu o Raport Kredytowy BIK.

Stworzony system antyfraudowy stanowi nową jakość w zakresie gromadzenia, przetwarzania i wykorzystywania gromadzonych danych na potrzeby współpracujących banków.

Udostępniony dedykowany do Systemu BIOR kanał automatyczny typu WebService pozwala korzystać z BIOR w sposób najbardziej automatyczny. Z jednej strony można automatycznie wprowadzać i aktualizować dane w BIOR, z drugiej jest możliwe automatyczne wyszukiwanie według zadanych kryteriów. Zapewnia to możliwość wykorzystywania zasobów zgromadzonych w BIOR w ramach wszystkich, nie tylko kredytowych, procesów weryfikacji danych klientów w bankach.

Według informacji pozyskanych od ekspertów Biura Informacji Kredy-

towej zakres uczestnictwa w zakresie Systemu antyfraudowego BIOR sukcesywnie się zwiększa. Na koniec 2013 r. w systemie uczestniczyło 15 banków, wprowadzono ponad 16 tys. danych.

O potencjalnej użyteczności rozwiązania niech przemówią liczby. W samym 2013 r. złożono ponad 1,2 mln zapytań do BIOR, głównie poprzez Raporty Kredytowe BIK.

W ramach tych zapytań znaleziono dane w BIOR dla wnioskowanych transakcji na ponad 47,8 mln zł, z czego:

- dla produktów ratalnych – ponad 11,5 mln
- dla produktów mieszkaniowych – ponad 34,1 mln
- dla produktów odnawialne – ok. 2,3 mln

W ramach podsumowania

Uwarunkowania formalnoprawne, techniczne i finansowo-organizacyjne sprawiają, że stworzony system antyfraudowy stanowi nową jakość w zakresie gromadzenia, przetwarzania i wykorzystywania gromadzonych danych na potrzeby współpracujących banków. Wzmacnia architekturę bezpieczeństwa i zarządzanie rodzajami ryzyka poprzez wykorzystanie gromadzonych wspólnie danych w czasie rzeczywistym, przy zachowaniu standardów i wymogów regulowanych odpowiednimi przepisami prawa i wewnętrznymi procedurami każdego z uczestników i beneficjentów systemu. W efekcie obok optymalizacji kosztów uzyskano efekt synergii polegający na wykorzystywaniu danych w sposób zoptymalizowany względem potrzeb i konkretnych zastosowań – w zależności od konkretnego procesu realizowanego w banku w ramach statutowej działalności. Od wielości uczestników systemu i ilości wprowadzanych przez nich danych zależeć będą dalsze perspektywy rozwoju systemu i korzyści dla jego uczestników. Dotychczasowe doświadczenia i uzyskane wyniki dowodzą, że przywołana zależność ma charakter wykładniczy i przekłada się na budowanie bezpieczeństwa sektora bankowego. ▀