Скорингові технології оцінювання ризиків шахрайства в банківській діяльності

© Кузнєцова Н.В.
Навчально-науковий комплекс «Інститут прикладного системного аналізу» Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
natalia-17@mail.ru

Анотація

У роботі розглянуто основні види ризиків шахрайства в банківській діяльності, такі як шахрайства при отриманні кредиту та зловживання з пластиковими картами. Розглянуто основні способи боротьби з ризиками шахрайства при отриманні кредиту, зокрема через побудову відповідних скорингових моделей та скорингових карт, що на етапі розгляду кредитних заявок відсіюють шахраїв. Для цього використовуються різні види скорингу: аплікаційний, поведінковий, скоринг щахрайських дій, колекшн-скоринг на різних етапах діяльності банку та строку кредиту. Для виконання будь-якого виду скорингу необхідні історичні дані (навчальна вибірка) для побудови скорингової моделі на основі логістичної регресії, мережі Байєса тощо. За допомогою розроблених скорингових моделей на етапі розгляду кредитних заявок здійснюється розділення позичальників на поганих (шахраїв) та «хороших», яким кредит може бути виданий. Розглянуто декілька видів шахраїв при отриманні кредиту: побутові, професійні тощо. Наведено загальний вид скорингової моделі для виявлення шахрайства та основні способи боротьби з шахраями, зокрема бюро кредитних історій, «чорні списки» тощо.

У роботі розглянуто також основні види махінацій з банківськими картами в Україні, такі як скімінг, фішинг, вішинг, які лише у 2016 році нанесли збитків більш ніж на 339 мільйонів гривень. Надано рекомендації для побудови фрейм-моделі кредитної картки для подальшого використання цієї моделі кредитної карти, та, відповідно, поведінки клієнта для виявлення шахрайських операцій і протидії ним. На прикладі операцій за кредитною картою показано, як існуючі спеціальні відділи моніторингу банківських карток можуть побудувати типову поведінку клієнту та банківської карти і, відповідно, відслідкувати нетипові операції, що здійснюються шахраями. Надано рекомендації для банку та клієнтів про спільну взаємодію шляхом своєчасного інформування та блокування шахрайських операцій і протидії скімінгу, фішингу та вішингу.

1 Вступ

Розвиток інформаційно-телекомунікаційних технологій за останні декілька років охопив майже всі куточки нашої планети; уявити світ без найсучасніших пристроїв зв'язку – мобільних телефонів, планшетів, ноутбуків, які за рахунок доступу до інтернету надають можливість залишатися на зв'язку і отримувати надзвичайно швидко і вчасно актуальну інформацію, просто неможливо. Поточні тенденції розвитку суспільства підсилюють потребу отримувати лише найнеобхіднішу інформацію за декілька секунд, не перевантажуючись супутньою інформацією, головним стає принцип доступу до інформації лише «одним натисканням пальцю». Зрозуміло, що не уся інформація про роботу підприємства має бути поширеною і доступною для користувачів; частина її є таємною або конфіденційною, і потрапляння такої інформації до відкритих ресурсів одразу робить її легкодоступною для зловмисників, які можуть використати її в подальшому у злочинних цілях. Зокрема, наразі в Україні дедалі зростає процент шахрайських дій зловмисників в банківській сфері. Це і махінації з пластиковими картками, і спроби отримання кредиту за неправдивими документами. Частка таких кредитів вже зараз становить більше 10%. Українські банки давно почали розробляти стратегію боротьби з такими зловмисниками, впроваджуючи так звані «чорні списки» таких клієнтів та розповсюджуючи цю інформацію через відкриті засоби та банки кредитних історій. Однак, незважаючи на розробку таких баз даних, це не знижує частку кредитних договорів, що не були повернуті.

2 Постановка задачі

Проблема протидії ризикам шахрайства в банківській сфері, які стали найпоширенішими в українській банківській діяльності протягом останніх років, у зв'язку зі значним розширенням використанням банківських карток і зростанням кількості осіб, що звертаються за кредитами. Один із шляхів розв'язання цієї проблеми – своєчасне виявлення і оцінювання ризиків шахрайства для індивідуальних клієнтів. Нагальною потребою є розвиток математичного апарату для розробки відповідних моделей, зокрема на базі скорингу.

3 Скорингові моделі та технології в українських банках

Особливо актуальною для банківської сфери сьогодні стало застосування спеціальних інформаційних технологій, які б дозволили виявити шахрайські плани зловмисників ще на етапі розгляду кредитних заявок. У такому сенсі важливою є задача ризик-менеджменту з розрізнення кредитних ризиків на шахрайства (fraud) та

дефолти (неможливість подальшого виконання своїх кредитних зобов'язань). Для цього українські банка використовують лише аплікаційний скоринг, що здебільшого пояснюється нерозвиненістю системи скорингу в Україні та високими цінами на послуги розробників скорингових моделей. За оцінюванням фахівців у типовій скоринговій моделі присутні від 10 до 30 параметрів: близько 10 – для споживчого кредитування та близько 30 – для автокредитування чи іпотеки. Звичайно, для повної та ефективної оцінки кредитоспроможності позичальника така кількість параметрів є недостатньою, відбираючи лише найвагоміші параметри при обчисленні кредитоспроможності кожного окремого позичальника [1].

Насправді світова практика використовує різні типи скорингу на різних етапах кредитування, а не лише етапі розгляду кредитної заявки, продовжуючи оцінювати вагу кредитної заявки впродовж всього життя кредиту, і навіть на етапі стягнення заборгованостей та передачі колекторам. На будь-яких етапах кредитної історії за допомогою скорингу можливе вирішення різноманітних завдань, таких як:

1. Скоринг за актуальними даними протягом оформлення заявки (англ. application scoring) – оцінка кредитоспроможності потенційних позичальників за наданою інформацією упродовж кредитної транзакції.
2. Скоринг протягом кредитного періоду (англ. behavioral scoring), коли оцінка динаміки стану кредитного рахунку позичальника дозволяє математично оцінити ймовірність повернення кредиту. Скорингові моделі ймовірності, що використовуються для цього, дозволяють спрогнозувати зміну платоспроможності позичальника, визначити оптимальні ліміти за кредитною карткою тощо.
3. Оцінка ймовірності повного або часткового повернення кредиту (англ. collection scoring) пропонує визначення пріоритетних напрямів роботи щодо позичальників, коли їхній кредитний рахунок класифікують як «незадовільний». Такий вид використовується за умов порушення позичальником зобов'язань щодо погашення кредиту. Згідно з результатами багатьох досліджень майже 40% неплатежів припадає на позичальників, які невимушено забувають внести платіж за кредитом. Підтримка скоринговою системою collection-скорингу дозволяє автоматично ліквідовувати цю заборгованість.
4. Оцінка можливості шахрайства (англ. fraud scoring) визначає ймовірність потенційних неправомірних дій позичальника. Як правило, цей метод використовується разом з аплікаційним і поведінковим скорингом вірогідного аналізу. Залежно від якості доступної інформації про позичальника і методу прийняття рішень скоринг поділяється на дедуктивний (англ. deductive credit scoring) і емпіричний (англ. empirical credit scoring) [2].

Зокрема, у комплексній системі управління кредитними ризиками SAS Credit Scoring for Banking існує аналітичний модуль формування моделей оцінки кредитоспроможності позичальників та їх сегментації та можливості формування алгоритмів та моделей виявлення шахрайства, тобто передбачені можливості виконання всіх видів скорингу для різних типів задач та для різних видів даних.

4 Аналіз шахрайських ризиків в Application Scoring

Шахраїв розділяють на три основні групи: «побутові» (індивідуали) шахраї, професіональні шахраї та позичальники, які використовують послуги професіональних шахраїв. Побутові шахраї не повертають кредит через матеріальні труднощі. Ці боржники не будуть ховатися від банку і колекторів, а після суду змушені будуть повернути товар і банки не отримують прибуток від таких кредитів. Самі клієнти будуть визнані фінансово нестабільними і потраплять в чорний список банку, кредитного бюро і не зможуть отримувати кредити в майбутньому. Професійні шахраї весь час змінюють адреси, мобільні телефони, ніде офіційно не працюють. Страждають від таких клієнтів навіть консервативні банки, де діє жорстка політика перевірки клієнтів та їх документів. Третім типом є позичальники, які залучають шахраїв для отримання кредитів для відкриття бізнесу і через якийсь час не в змозі повернути кредит, і врешті-решт самі стають шахраями. Менша частина таких клієнтів – це люди, які співпрацюють з шахраями, що виготовляють неправдиві документи, і ділять з ними прибуток від шахрайства [3, 4].

Збитки, які отримує банк внаслідок шахрайських дій зловмисників буде залежати від «вартості» шахрайського кредиту та відповідно кількості таких кредитів. Для банку розраховуються так звані очікувані втрати, EL від прояву різних видів фінансових ризиків для підприємства за наступною формулою:

$$EL = \sum_{i=1}^{N} P(R_i) \cdot CE_i \cdot LGD_i, \qquad (1)$$

де $P(R_i)$ – ймовірність (очікувана частота) прояву і-го виду ризику (наприклад, ризику зниження фінансової стабільності), що набуває значення на відрізку [0,1]; CE – загроза внаслідок реалізації ризику – сума втрат (заборгованості внаслідок реалізації даного ризику); LGD – покриття ризику страховкою (в разі її наявності) заставою або ефективність запобіжних засобів, що приймає значення від 0 (ризик повністю покритий заставою) до 1 (ризик не покритий заставою); N – кількість ризиків.

Найбільш цікавим показником є ймовірність дефолту. В основному всі дослідження щодо оцінки кредитного ризику ведуться саме в напрямі розробки механізму розрахунку ймовірності дефолту. На основі певних параметрів позичальника та кредиту x_i^j необхідно розробити процедуру оцінки ймовірності дефолту PD_i [5]:

$$PD_i = F(w^j, x_i^j),$$

де w^j – ваги параметрів x_i^j, i – кількість позичальників, j – кількість параметрів кредиту .

Наприклад, скорингова модель оцінки кредитоспроможності індивідуального позичальника на основі мереж Байєса описується наступною формулою:

$$PD = F(v^k, G, J) = \underbrace{\sum_s ... \sum_r}_{k} p(v_s^1, ..., v_r^k) \cdot p(D \mid v_s^1, ..., v_r^k) = 1 - PR_i ,$$

де v^k – батьківські змінні, що впливають на змінну неповернення кредиту;

J – імовірнісний розподіл змінних v^k; G – спрямований ациклічний граф, вузли якого відповідають випадковим змінним v^k модельованого процесу; v_r^k – стани змінної v^k, v_s^1 – стани змінної v^1; $k < j$.

Скорингова модель у вигляді логістичної регресії може легко та зручно застосовуватись як для прогнозування дефолту (1– дефолт, 0 – повернення кредиту), так і для прогнозування шахрайськийх дій (1 – шахрайські дії, 0 – добрий позичальник) , оскільки представлена в наступному вигляді:

$$y = F_3(x_k) = \frac{\exp(\beta_0 + \beta_1 x_1 + ... + \beta_k x_k)}{1 + \exp(\beta_0 + \beta_1 x_1 + ... + \beta_k x_k)}, \quad k < n .$$

Засобом зниження кредитних ризиків від шахрайства, особливо для продуктів без застави, є формування та використання моделей виявлення шахрайства Application Fraud Scoring. Застосування аналітичного модуля SAS для формування таких моделей допомагає банку створити послідовну і логічну базу для прийняття рішень, надати працівникам кредитного відділу більш чітку інтуїтивно зрозумілу міру кредитного ризику (рис.1).

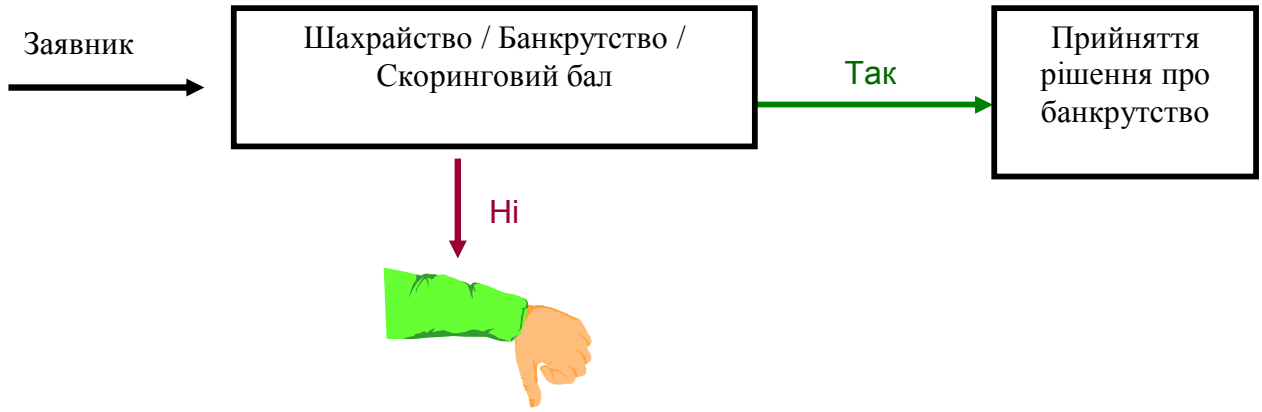

Рис.1. Аналіз та виявлення шахрайських дій в SAS Credit Scoring for Banking

Процес скорингового оцінювання може бути представлений у вигляді послідовності кроків:

1) за затвердженою банком скоринговою моделлю на основі анкетних даних заявника та даних по кредиту здійснюється розрахунок скорингового балу клієнта та перевірка його на схильність до шахрайства або банкрутства:

$$Score_i > ApprovalRateMin ,$$

де $Score_i$ – скоринговий бал, розрахований для і-го позичальника розробленою скоринговою моделю.

$ApprovalRateMin$ – поріг, що встановлюється банком як мінімальне допустиме значення скорингового балу, при перевищенні якого кредит видається позичальнику. Залежно від політики банки та ситуації на ринку поріг може змінюватися.

2) якщо скоринговий бал заявника менше від порогового балу у банку, то приймається рішення про банкрутство. Якщо з'являються свідчення щодо шахрайських або нетипових дій, то приймається рішення щодо відпрацювання дій по запобіганню шахрайству – передається інформація у відповідні органи та інші банки для виявлення та пошуку зловмисника.

В результаті оцінки історичних даних (навчальної вибірки) формується кредитний портфель потенційного позичальника, що дозволяє розділяти потенційних позичальників на поганих (шахраїв) та «хороших», яким кредит може бути виданий. Цей результат закладається в історичний файл (навчальну вибірку) цільової змінної (target) і будується модель та профіль шахрая. Таким чином претенденти на отримання кредиту ранжуються за групами, кожній з яких присвоюється характеристика надійності позичальника від «високої» до ризикової (шахрай). Зазвичай, оцінка кредитного скорингу шахрая будується на основі 10-12 базових параметрів – сімейний стан, наявність персонального автомобіля, частота зміни роботи, тривалість проживання за останнім місцем тощо. Виходячи з результатів, отриманих за цими критеріями (частина інформації отримується з анкети клієнта, але потім уточнюється та перевіряється службою безпеки банка), система виставляє потенційному клієнту певну кількість балів. Далі в автоматичному режимі співставляє отриману оцінку із заданим порогом відсікання. Клієнти, у яких оцінки виявились нижчими за

порогове значення, не зможуть стати позичальниками банку. Аналіз кредитного скорингу (Score Fraud) дозволяє оцінити профіль шахрая і використовувати його на етапі прийняття рішення про видачу кредиту. Після проведення оцінки ймовірності шахрайства застосовуються традиційні моделі та скорингові карти для оцінки кредитоспроможності позичальника і ймовірності дефолту.

В разі виявлення скоринговою моделлю шахрайських факторів, тобто співпадіння характеристик, що відповідають характеристикам зловмисників, інформація про такого позичальника перевіряється через доступні бюро кредитних історій на предмет співпадіння з відомими шахраями, які могли змінити персональні дані (підробити), місце проживання і вже розшукуються за скоєні зловмисні дії. У разі співпадіння інформація терміново передається службі безпеки та правоохоронним органам для проведення подальшого розслідування.

Ще однією можливістю для вчинення шахрайських дій залишається потрапляння до зловмисників інформації про особливості самої скорингової моделі, яка використовується на даний момент в банку для перевірки платоспроможності позичальників та відібраних характеристик, порогу відсікання тощо. Така інформація може передаватися шахраям безпосередньо працівниками банку. Засобом боротьби з таким видом ризику є підвищення безпеки скорингової моделі, періодична перевірка працівників банку, та періодичне оновлення скорингової моделі та відповідно скорингових карт для поведінкового скорингу та скорингу потенційних позичальників.

Аналізуючи статистичні дані декількох українських банків, можна зробити висновок, що шахрайські дії зловмисників, які не були виявлені на етапі fraud скорингу, в подальшому будуть спостерігатися в якості постійної прострочки платежів, починаючи з першого місяця сплаті по кредиту. Всі дії, які спрямовуються банками на повернення такого кредиту (повідомлення, дзвінки тощо) є нерезультативними, бо скоріш за все в цей момент шахраї вже змінюють адреси проживання та мобільні телефони. Таким чином, єдиним ефективним способом боротьби з шахрайством при отриманні кредиту є розробка коректної скорингової моделі – скорингової карти – яка дозволить працівникам банку виявити фактори, що характеризують шахраїв, і відмовити у видачі кредиту.

На жаль, ще одним фактором підвищення ризиків шахрайства в банку залишається той факт, що прийняття рішення щодо видачі кредиту здійснюється самими працівниками фінансових установ після отримання автоматичного результату оцінювання за скоринговою картою. Тут залишається можливість маніпуляції та видачі кредиту тим особам, яким скорингова система відмовила в отриманні кредиту (наприклад, через наявність заборгованостей в інших банках чи негативної кредитної історії в бюро кредитних історій). Для уникнення людського фактору при прийнятті кредитних рішень рекомендується автоматизувати повністю процес прийняття рішень при аналізі кредитних заявок і забезпечити неможливість або складність зміни прийнятих рішень (наприклад, через штрафні санкції для працівників банку в разі виявлення кредитів, по яким приймалося рішення всупереч скоринговій карті, і по яким встановлені факти заборгованості або неповернення кредитів).

5 Махінації та зловживання з пластиковими картками в Україні

Ще одним типом шахрайських дій в банківській сфері є маніпуляції з пластиковими картками, тобто незаконне вилучення зловмисниками коштів шляхом різного роду дій з банкоматами, зокрема скімінг, трапінг, фізичне пошкодження банкоматів тощо, а також такі, що пов’язані з використанням комп’ютерних технологій та Інтернету – фішинг, вішинг, різного роду віруси, хакерські атаки та ін. За принципом поширеності можна виділити такі типи шахрайств (табл. 1) [6].

Табл. 1. Класифікація шахрайств за принципом поширеності

Типи шахрайств	Частка поширеності шахрайства (%)
1. Шахрайство з втраченими і викраденими пластиковими картками	72,2
2. Шахрайство з підробленими картками	20,5
3. Шахрайство з картками, не отриманими законним держателем	2,8
4. Шахрайство з використанням рахунку	1,4
5. Інші форми шахрайств	3,1

За даними Національного банку України у 2016 році в Україні 31,1 млн. активних банківських карток. Українська міжбанківська асоціації членів платіжних систем (ЄМА) [7] у 2016 від шахрайства постраждало 1,22% користувачів-власників платіжних карт, причому частка вішингу та фішингу разом склала 63%, а загальна сума збитків склала 339,13 мільйонів гривень, з них від вішингу – 275,45 млн., фішингу – 63,68 млн. гривень, що склало більш ніж в чотири рази більше у порівнянні з сумою збитків у 2015 році – 84,36 мільйонів гривень. Рекордно зросла і кількість фішингових сайтів (з 38 до 174 сайтів), список яких постійно оновлюється та доповнюється на сайті ЕМА. Жертвами телефонних махінацій стали 0,63% власників банківських карток, що в 3 рази більше порівняно з 2015 роком.

Порівняно з 2015 роком збільшилась і середня сума шахрайських операцій, зокрема для вішингу з 834 до 1403 гривень, фішингу – з 206 гривень до 345. Проте зменшилась кількість випадків махінацій з банкоматами: компрометація даних (скімінг та івсдропінг) – з 99 до 71 у 2016 році, випадки захоплення готівки (кеш-трепінг) з 991 до 830, а кількість незаконних операцій з банківськими картками перевищило 57 тисяч.

Рис.2. Обсяги шахрайства з банківськими картками в Україні за інформацією ЄМА [7]

Кредитна карта – платіжна банківська карта, що дозволяє її держателю отримувати товари та послуги на підставі обіцянки оплатити покупки. Емітент карти (зазвичай банк) створює револьверний рахунок та надає лінію кредиту власнику, з якого він може позичати гроші для оплати комерційних послуг або для зняття готівки.

Револьверний кредит (англ. revolving credit) (РК) – автоматично поновлюваний (від лат. revolve – обертатись) кредит, який широко використовується у світовій практиці на ринку позичального капіталу. РК надається без додаткових переговорів між позичальником і банком, якщо сума кредиту не перевищує встановленого ліміту та строків погашення. У цьому відношенні РК схожий на кредитування на основі кредитної лінії, хоча й має суттєві відмінності. Сторонами в угоді про надання РК. можуть бути уряди, міжнародні організації, групи банків, підприємства та фізичні особи. РК надається, як правило, позичальникам, які мають постійні відносини з банком, якісну кредитну історію, або під надійні гарантії. Прикладом РК. можуть бути кредити за кредитними картками та за єдиним активно-пасивним поточним рахунком у формі овердрафту, певні кредитні лінії. Клієнт банку в разі нестачі власних коштів може скористатися РК без попередження банку і без оформлення додаткових документів, але в межах обумовленого угодою ліміту кредитування. РК погашається в міру надходжень коштів на рахунок клієнта. Погашення заборгованості відновлює вільний ліміт кредитування та автоматично продовжує право користування РК [8].

Для аналізу поведінки клієнтів потрібно виділити основні параметри КК, які б найбільш повно описували її природу та функції. Найпростіша модель кредитної картки включає в себе дату видачі (beginDate), дату закінчення договору (finishDate), що зазвичай складає 1-2 роки, та дату фактичного закриття договору (closeDate). Також є можливість встановити ліміт – права на це має емітент карти, та дізнатися його величину в даний момент. Однак потрібно врахувати можливість взяття в кредит певної кількості грошей, що не перевищує встановленого ліміту (setLoan()). На основі величини цього кредиту розраховується мінімальний щомісячний платіж (getPayment()), якщо на кінець місяця він не буде здійснений в повному обсязі, то залишок платежу стає заборгованістю, а сам платіж вважається простроченим. Тому потрібна реалізація можливості перегляду цієї заборгованості (getOverdue()). Як правило, процентна ставка для простроченої заборгованості значно більша за основну і при наступному внесенні коштів, гаситься саме вона. Згідно з цими зауваженнями більш детальна модель КК, що і буде використовуватися надалі має вигляд, наведений у табл. 2.

В основу моніторингу кредитної карти та відслідковування шахрайських дій може бути покладена середньостатистична модель поведінки клієнта, що характеризується рядом параметрів, відхилення від яких система онлайн-моніторингу може сприймати як шахрайство і відмовляти у проведенні операції. Проте побудова адекватної статистичної моделі поведінки клієнта вимагає значного часу і великих обчислювальних ресурсів. Відповідно до цього для вирішення завдання запобігання шахрайства доцільно передавати частину функцій управління ризиками безпосередньо власникам карток. На стадії випуску і функціонування картки її власник зможе сам визначати стандартну для себе модель поведінки. Для цього банк повинен забезпечити власника картки можливістю оперативно змінювати параметри моделі її використання: кредитні ліміти, кількість операцій в день, можливість виконання операцій в Інтернеті, платежі закордоном тощо. Такий підхід вимагає з боку банку певних ресурсних витрат на доопрацювання програмного забезпечення, розробку нових технологій з управління параметрами картки, доопрацювання програмного забезпечення кол-центру (call-center). Велике значення для протидії шахрайським операцій з боку банку є забезпечення клієнта цілодобовим

доступом до кол-центру та можливістю оперативно, за запитом, отримувати інформацію про стан рахунку, оперативно блокувати / розблоковувати картку, оперативно отримувати інформацію про проведення / спроби проведення операцій.

Табл. 2 Модель кредитної карти

Слоти	Опис
beginDate	Дата початку
finshDate	Дата номінального закінчення
closeDate	Дата фактичного закінчення
gracePeriod	Грейс-період
setLimit()	Встановлення ліміту
getLimit()	Перегляд поточного ліміту
Balance	Баланс
postDuePayments	Кількість прострочених платежів
setLoan()	Надання кредиту
getOverdue()	Отримання величини прострочки
getOutstanding()	Отримання величини термінової заборгованості
getPayment()	Отримання щомісячного мінімального платежу

Розглянемо приклад моніторингу кредитної карти за описаною вище моделлю, коли відбувається підвищення кредитного ліміту в певні періоди (рис.3).

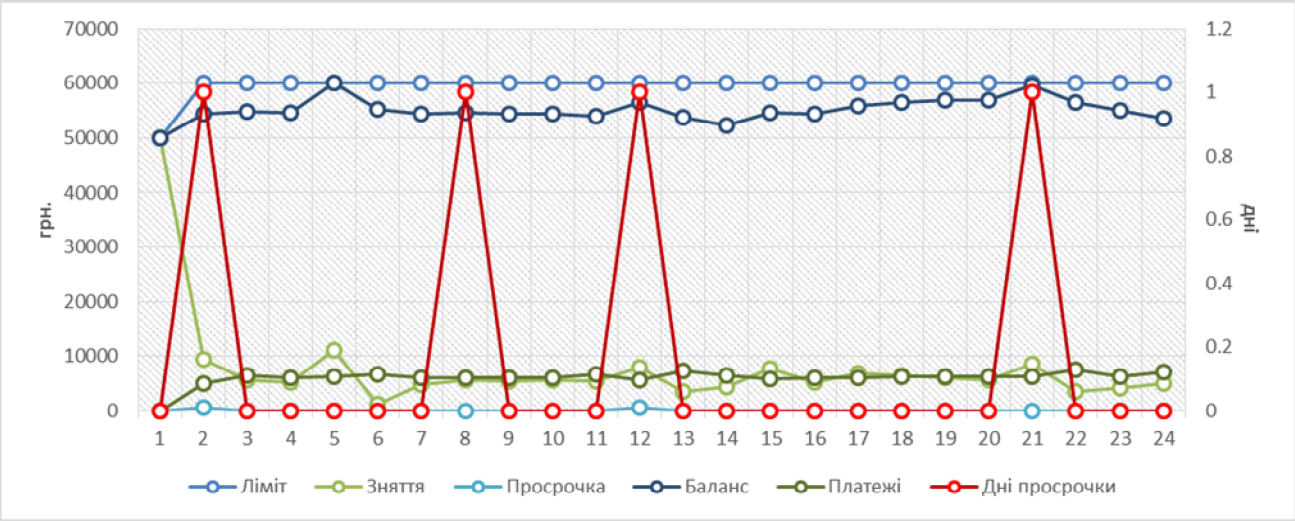

Рис. 3. Моніторинг кредитної карти із збільшенням ліміту в певні періоди

Якщо підняття ліміту відбувається в перший раз, то банку необхідно відслідкувати таку операцію, зв'язавшись додатково з клієнтом та перевірити, що операції проводяться саме клієнтом, а не шахраєм. У подальшому, моніторинг банківських карт буде мати модель поведінки банківської карти, періодичністю і навіть сумою сплати щомісячно банківською картою і у подальшому зможе моніторити лише підозрілі нетипові операції.

Введення обмежень на використання картки самим клієнтом в значній мірі підвищує ефективність роботи систем офлайн-моніторингу банку і дозволяє без фінансових втрат на ранній стадії виявити випадки підробки карток. Заходи щодо мінімізації ризиків при обслуговуванні торгово-сервісної мережі полягають в реалізації комплексу організаційних і технологічних процедур, спрямованих на обмеження можливості проведення несанкціонованих платежів і створення стійкого непривабливого іміджу торгово-сервісної мережі банку для шахраїв.

Процедура моніторингу та протидії шахрайства суттєво залежить від самого банку та системи моніторингу операцій, яка у ньому розроблена. Швидке збільшення кількості та різноманітність шахрайських атак змушують банки безперервно адаптувати систему моніторингу та протидії шахрайських дій. Зловмисники викрадають як особисті дані клієнтів (фішинг, шиммінг), так і самі банківські картки карти (скімінг). Останнім часом почастішали випадки надсилання повідомлень на мобільні телефони з вимогою підтвердження певної торгівельної операції (яка насправді не проводилась карткою), а після цього дзвінка начебто співробітника банка, який заявляє про підозрілу операцію і для її блокування необхідність надати дані картки, зокрема 3 останні цифри зі зворотного боку картки, що дозволяють здійснювати списання коштів в Інтернет.

В українських банках довгий час існувала практика добровільно-нав'язувального принципу страхування банківських карток та їх клієнтів від фінансової відповідальності в разі вчинення з картою певних шахрайських дій. Це означало, що якщо з карти будуть списані гроші зловмисниками, то вся сума буде повернута клієнту на рахунок. Така послуга страхування фінансових ризиків пропонувалась власникам

дебітних карток, а для власників кредитних карток майже всюди була підключена за замовчуванням, передбачаючи щомісячну сплату за таку послугу від 10 до 15 гривень. Ситуація дещо змінилась з 1 серпня 2016 року, коли найбільша міжнародна платіжна система Visa ввела обов'язковий принцип «нульовий відповідальності» для власників своїх карток. Для банків це означає, що на практиці всі шахрайські операції, в результаті яких клієнт втратить гроші, доведеться покривати саме фінансовими установам. Цей принцип не є новим і чим-то надзвичайним, адже це стандартна практика платіжної системи в усіх країнах з якими вона співпрацює. В українських банках про такі принципи були проінформовані завчасно, але ситуація з зобов'язанням клієнтів самостійно відповідати за свої гроші на картках або страхуватися, в принципі не змінилась. З 1 серпня механізм особливо не змінився - в разі пропажі коштів банк проводить розслідування на предмет причетності клієнта до шахрайства. І потім вже сам приймає рішення, відшкодовувати кошти чи ні. У кожному серйозному банку існує підрозділ моніторингу шахрайства, який при виникненні випадків шахрайства детально перевіряє всі обставини і за кілька місяців (офіційно розгляд питання може становити до півроку) приймають рішення та, відповідно, після цього банк повертає кошти клієнтам.

Тому зараз, в умовах підвищеного ризику банки, давно практикують SMS і email-інформування клієнтів, недавно впровадили перевірка 3D-secure - це додаткова ідентифікація для інтернет-платежів. Крім цього, банки пропонують спеціальні картки для розрахунку в Інтернеті (інколи вони є навіть віртуальними) з підвищеним рівнем захисту. На таку карту можна встановити різні обмеження, починаючи від кількості транзакцій і закінчуючи сумою операцій і транзакції, що відбуваються в Інтернеті відслідковуються банком набагато уважніше.

Насправді більшість банкірів зазначають, що питання відшкодування витрат клієнтам мають вирішуватися на законодавчому рівні. Тобто, передбачити в законодавстві єдину умову, що при зверненні клієнта про шахрайські дії з його рахунками, банк спочатку відшкодовує втрачені кошти клієнту, а вже потім проводить розслідування, правомірно було списання або був факт шахрайства. Причому на законодавчому рівні відповідно до Конституції України такі умови мають діяти для всіх клієнтів українських банків, незалежно від того, яким банком і якою платіжною системою був відкритий рахунок чи була виготовлена картка.

6 Висновки

Останні декілька років в Україні надзвичайно швидкими темпами розвивалися різні види кібер-злочинності та шахрайських операцій. Якщо збитки від шахрайських дій під час отримання кредиту несуть лише самі банки, то зрозуміло, що саме банки зацікавлені і розробляють різні види скорингових моделей для виявлення всіх типів махінацій на різних етапах отримання та обслуговування кредиту. В цій сфері напрацьовано різноманітні способи боротьби з побутовими та професійними шахраями, передбачене вже регулювання і підтримка з боку держави. Зокрема, існуючий механізм бюро кредитних історій та бази кредитних історій (а їх в Україні декілька, і за інформаційний запит по кожній особі чи знаходиться вона в «чорному списку» банк сплачує від 10 до 20 гривень), куди потрапляли недобросовісні позичальники та шахраї був використаний для розробки Міністерством юстиції України так званого реєстру боржників. Цей реєстр запущений лише в цьому році і туди будуть потрапляти українці, які мають борги за комунальні послуги, проблемні кредити, запідозрені в шахрайстві, та ті, що не повернули позику. Таким «чорним списком» можуть користуватися кредитні спілки, банки, фінансові установи, які зацікавлені в інформації щодо платоспроможності своїх клієнтів. Ще одним дієвим механізмом боротьби з шахраями та особами, що не повертають кредит, став розроблений спільно з Кабінетом Міністрів механізм обмеження виїзду закордон шахраїв та боржників. Саме такі особи перевіряються нашою прикордонною службою на предмет існування заборгованостей, або просто перебування цієї особи в «чорному списку» і може стати причиною для затримання такої особи на кордоні.

Для боротьби з шахрайськими діями в банківській сфері створено спеціальну кіберполіцію, профільні комітети, спеціальні громадські та міжбанківські асоціації, які з одного боку, напрацьовують єдині моделі виявлення шахрайських дій, обмінюються та постійно оновлюють інформацію щодо існуючих способів та сайтів для викрадення даних з банківських карток. З іншого боку, проводять інформаційно-просвітницьку діяльність, попереджаючи клієнтів-власників банківських карт про неприпустимість передачі особистих даних стороннім особам. Самі банки розробляють механізми моніторингу та відслідковування підозрілих операцій. Якщо зазвичай клієнт виконає всі платіжні операції в одному конкретному місті, але раптом операція відбувається де-небудь в іншому куточку світу, то такі транзакції мають банками заблокуватися автоматично і запросити додатково підтвердження клієнта, наприклад дзвінка на мобільний телефон або надсилання смс.

Слід зазначити, що швидкий розвиток інформаційних технологій спричиняє появу надзвичайно великої кількості нових видів махінацій в банківській діяльності, способів боротьби з існуючими механізмами протидії шахрайству у банках. Тому основним способом боротьби з шахраями є постійне оновлення скорингових моделей виявлення шахрайства, зміни їх параметрів, підвищення швидкодії моніторингу операцій, нарощення ІТ-засобів та тісна співпраця з кіберполіцією. У роботі запропоновано використання скорингових моделей та спецільних скорингових технологій для виявлення шахрайських дій ще на етапі розгляду кредитної заявки або при спробі несанціонованого отримання грошей з банківських карток.

Література

1. Бучко І. Є. Скоринг як метод зниження кредитного ризику банку / І. Є. Бучко // Вісник Університету банківської справи Національного банку України. – 2013. – Випуск 2 (17). – С. 178–182.
2. Narain B. Survival analysis and the credit granting decision / B. Narain // Credit Scoring and Credit Control. – 1992. – No. 1. – P. 1-2.
3. Кузнєцова Н.В. Аналіз фінансових ризиків з використанням SAS-технологій обробки даних / Н. В. Кузнєцова, П.І. Бідюк // Електротехнічні і комп'ютерні системи. – 2016. – № 22(98). – С. 267 – 271.
4. Siddiqi N. Credit Risk Scorecards: Developing and Implementing Intelligent Credit Scoring /N. Siddiqi// John Wiley & Sons, Hoboken. – 2005. – 208 p.
5. Бідюк П. І. Моделі оцінки ризиків кредитування фізичних осіб / П. І. Бідюк, Є. О. Матрос // Кібернетика та обчислювальна техніка. – 2007. – №153. – С. 87–95.
6. Харчук М.В. Аналіз масштабів та основні напрями мінімізації ризиків шахрайства членів міжнародних платіжних систем / М.В. Харчук //Ефективна економіка. – №6, 2013. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=2120.
7. Сайт Української міжбанківської асоціації членів платіжних систем [Електронний ресурс]. – Режим доступу: https://ema.com.ua/.
8. Міщенко В. І. Банківські операції: підручник / В. І. Міщенко, Н. Г. Слав'янська, О. Г. Коренєва.// Київ: Знання, 2007. – 280 – 283 с.

Scoring Technology for Risk Assessment of Fraud in Banking

© Nataliia V. Kuznietsova
Educational-Scientific Complex "Institute for Applied System Analysis" National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
natalia-17@mail.ru

Abstract

The paper describes the main types of risks of fraud in banking activity such as fraud in obtaining credit and abuse credit cards. The main ways for decreasing of fraud risk in obtaining credit, particularly through the building of appropriate scoring models and scoring cards are discussed. They cut off the frauds on the stage of the loan applications. It is used the different types of scoring: application, behavioral, collection and fraud-scoring at different stages of the bank activity and term of loan. It is needed for each type of scoring to have historical data (study sample) for building a scoring model based on logistic regression, Bayesian networks and others. Developed scoring models give the opportunity to separate bad borrowers(scam) and "good" on the stage of credit applications. Several types of fraudsters in obtaining credit, domestic, professional are considered. An overall view of a scoring model for fraud identification and main ways to combat fraud, credit bureau, "blacklists" is described.

The paper also reviews the main types of fraud with bank cards in Ukraine such as skimming, phishing, vishing, so that only in 2016 caused the loss of more than 339 million UAH. Recommendations for frame credit card model building for further using of this credit card model and its holder behavior to identify fraudulent transactions and combating them. On example of credit card transactions it is shown how existing bank cards monitoring departments can build client behavior and banking cards and, consequently, to track unusual transactions scams. There are given in the paper the recommendations for the bank and clients on joint cooperation through timely information and block such fraud actions as skimming, phishing and vishing.