УДК 343.72:336.77

Лінда Деламайре (Великобританія), Хуссейн Абдоу (Великобританія), Джон Пойнтон (Великобританія)

Шахрайство з кредитними картками та способи виявлення: аналіз

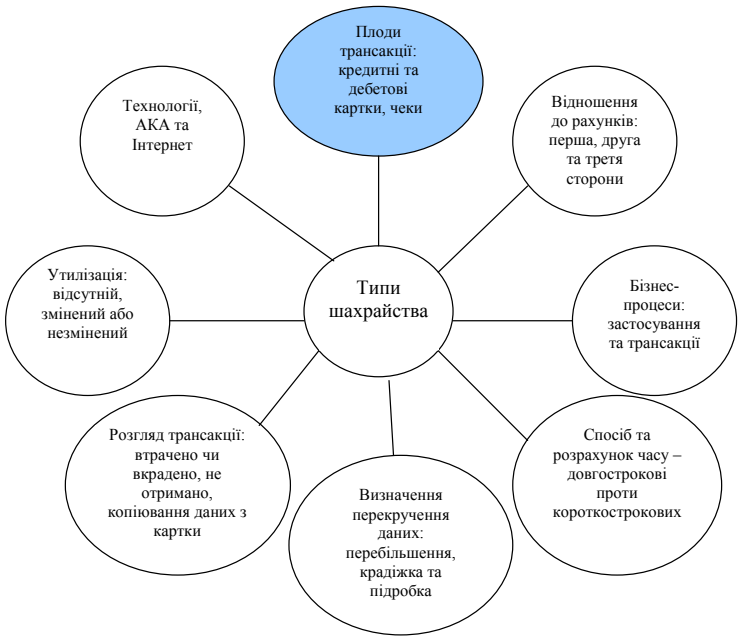
Шахрайство є одним з питань етики в секторі виготовлення кредитних карток. Цілями статті є визначення різних видів шахрайства з кредитними картками, розгляд альтернативних способів виявлення шахрайства, пропозиція, порівняння та аналіз нещодавно оприлюднених результатів розслідувань на предмет виявлення шахрайства з кредитними картками. У статті розглянуто загальні умови у сфері шахрайства з кредитними картками та виділено головні статистичні й кількісні дані. Залежно від виду шахрайства, з яким стикаються банки або компанії, що працюють з кредитними картками, можуть бути вжиті різні заходи. Стаття містить корисні пропозиції стосовно зниження витрат та часової ефективності. Важливість застосування методів, які тут розглядаються, полягає у зменшенні шахрайства з кредитними картками. Однак трапляються випадки, коли справжні замовники кредитних карток неправильно класифікуються як шахраї.

Ключові слова: шахрайство з кредитними картками, способи виявлення, бюро кредитної інформації, способи аналізу даних.

Вступ

Упродовж тривалого часу науковці виказували зацікавленість етичними питаннями банківських операцій (Молінекс, 2007; Джордж, 1992) та моральною складністю обману (Кларк, 1994). Шахрайство означає отримання послуг/товарів і/або грошей у неетичний спосіб і є наразі великою проблемою у всьому світі. Шахрайство стосується випадків, коли мають місце злочинні наміри, які, зазвичай, важко визначити. Кредитні картки є однією з найпоширеніших цілей шахрайства, але не єдиною; шахрайство має відношення до кожного виду кредитних продуктів, таких як особисті позики, житлові кредити і торгівля в роздріб. Більш того, природа шахрайства радикально змінилася за останні кілька десятиліть, що пояснюється зміною та розвитком технологій. Критичним завданням у плані допомоги промисловим підприємствам та фінансовим установам, включаючи банки, є вжиття заходів для попередження шахрайства, а також ефективної боротьби з ним (Андерсон, 2007).

Андерсон (2007) дав наступне визначення різних видів шахрайства (рис. 1).



Джерело: Власний графік автора на основі класифікації Андерсона (2007).

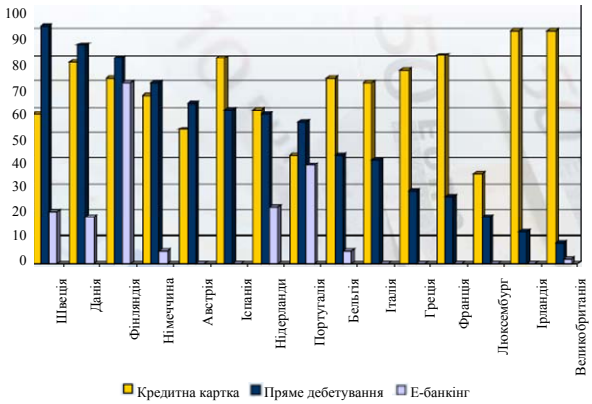
Рис. 1. Види шахрайства

Автори вдячні Пітеру Сінклеру за цінні поради та Pago e-Transaction Services GmbH за всі дані, використані у цій статті.

Основними цілями статті є визначення різних видів шахрайства з кредитними картками і розгляд альтернативних способів, що використовуються у виявленні шахрайства. Акцент робиться на Європу, тому етичні питання інших культур не беруться до уваги. Насправді, продукти операцій, включаючи кредитні картки, є найбільш уразливими по відношенню до шахрайства. З іншого боку, такі продукти, як персональні позики і торгівля в роздріб, також перебувають під ризиком і, крім того, мають серйозне етичне значення для банків та компаній, що працюють з кредитними картками. Шахрайство з кредитними картками може здійснюватись у різні способи, що залежить від виду шахрайства; це формує шахрайство банкрутства, шахрайство крадіжки/ шахрайство підробки, шахрайство звертання за кредитом і поведінкове шахрайство. Кожна з цих підкатегорій має власне визначення і специфіку. У статті розглянуто способи боротьби з ними та запропоновано приклади з європейських ринків.

Аналітики агенції Euromonitor International (2006) заявили, що 120 мільйонів карток (а саме, дебетові, кредитні та платіжні картки) використовувались у 2004 році в Німеччині, і що загальна ринкова вартість, створена цими картками, досягла 375 млрд. євро у 2004 році, що перевищує показник 2003 року більш ніж на 4%. У зв'язку зі збільшенням використання карток для здійснення платежів сума, витрачена на продаж та Інтернет-закупки з картками будь-якого виду сягнула 5% (170 млрд. євро). Однак отримання грошей з банківського рахунку стало менш популярним. Виникнення нових видів оплати пов'язане, можливо, з тим, що клієнти замінюють готівкові розрахунки на карткові (Euromonitor International, 2006).

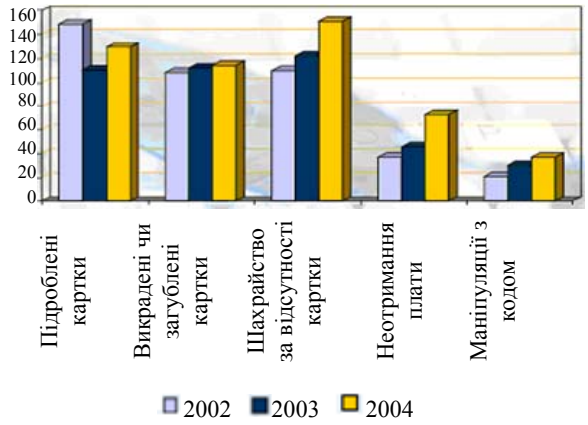
Якщо зосередитись на питанні кредитних карток у Німеччині, то тут, наприклад, слово "Kreditkarte" стосується платіжних та кредитних карток. Між ними немає чіткого розмежування, тоді як в англійців різні продукти мають власні терміни. Щоб розрізняти ці два продукти, дебетова картка та кредитна картка, банки, що працюють з кредитними картками, надають своїм клієнтам можливість поновлювати кредити через кредитні картки. Ця послуга є одним зі шляхів їх приваблення. Однак, навіть якщо клієнти можуть поновити кредит, не всі з них використовують таку можливість. У 2004 році кредитні картки набули більшої популярності, ніж платіжні картки (Euromonitor International, 2006).



Джерело: Промова в Амстердамі 19 квітня 2005 року.

Рис. 2. Продукти в обігу у Європі

У 2005 році, як показано на рисунку 2[1], ринок продуктів в обігу у Європі поділено на дві групи. Група кредитних карток, яка веде ринок, включає наступні країни: Іспанію, Бельгію, Італію та Грецію. У двох країнах, Сполучене Королівство та Ірландія, кредитні картки не мають конкурентів у показниках продуктів в обігу. Інша ж група країн використовує переважно дебетові картки; це можна сказати про Швецію. Однак, якщо говорити про всю групу, стандартне відхилення між двома видами продуктів в обігу є менш видимим, ніж для іншої групи. Німецький ринок, наприклад, недостатньою мірою використовує кредитні картки. Хоча протягом останніх декількох років сплачування картками тут набуло значних обертів. Прогнозується, що ринок для кредитних та платіжних карток зріс до 23.3% у період з 2004 по 2009 рік, досягши 56,477 млн. євро (Euromonitor International, 2006).



Джерело: Промова в Амстердамі 19 квітня 2005 року.

Рис. 3. Розподіл шахрайства у Європі

Шахрайство є головною проблемою у сфері кредитних карток. У Європейському Союзі перші його ознаки були помітні у Великобританії у 90-х роках. Насправді, загальні втрати через шахрайство з кредитними картками швидко зростали (1997 – 122 млн. фунтів стерлінгів;

1998 – 135 млн.; 1999 – 188 млн.; 2000 – 293 млн. фунтів стерлінгів (Асоціація систем клірингових платежів (APACS), без дати). Однак у 2006 році APACS оголосила про збитки на суму 423 млн. фунтів стерлінгів (спад близько на 80 млн. фунтів за останні два роки). Головною причиною цього покращення є успіх карток з авторизацією за пін-кодом (chip & PIN), що привело до зменшення заочного шахрайства. Однак тоді як кількість випадків шахрайства із загубленими та викраденими картками зменшується, число підроблених карток збільшується (APACS, без дати).

Складність шахрайства з кредитними картками полягає в тому, що воно може здійснюватись у різні способи, як то крадіжка, неправильне використання та банкрутство. У 2005 році (рис. 3) на європейському ринку домінували шахрайства викрадення та підробок. Але не акцентуючи уваги на запобіганні шахрайству або його виявленні, ризиком для банку може виявитись те, що "шахрайство з кредитними картками, зазвичай, залишається невиявленим упродовж тривалого часу вже після того, як вчинено злочин" (Камінер, 1985; Болтон і Ханд, 2001). Отже, це створить невідшкодовані збитки для банку.

У статті запропоновано заходи зі зменшення очікуваних витрат. У першому розділі визначено основні поняття, які використовуються у контексті шахрайства, з поясненнями. У розділі 2 розглянуто основні види шахрайства з кредитними картками. Розділ 3 містить обговорення способів виявлення. Насамкінець запропоновано висновки.

1. Поняття

Кредит є методом продажу товарів або послуг у випадку, коли покупець не має готівки на руках. Кредитна картка – це єдиний автоматизований шлях надання кредиту клієнту. Сьогодні кожна кредитна картка має ідентифікаційний номер, що прискорює торгівельні операції. Згідно з даними енциклопедії Британіка (без дати), "використання кредитних карток почалось у Сполучених Штатах у 1920-х роках приватними фірмами, нафтовими компаніями та готельними мережами". Однак згадки про кредитні картки зустрічаються ще в 1890-х у Європі. Перші кредитні картки включали покупки напряму між купцем, що пропонує кредит та кредитну картку, та його клієнтом. У 1938 році компанії почали приймати картки одна в одної. Сьогодні кредитні картки дозволяють робити покупки з необмеженою кількістю третіх осіб (Беліс, без дати).

У Європі найвідомішими компаніями з випусну кредитних карток є Barclaycard, Citibank та American Express, які пропонують різні види продуктів. Залежно від продукту, що пропонується, послуги, пов'язані з карткою, можуть бути різними. Процентна ставка, карткові сплати, плата валютного курсу, комісія за прострочку, кредитний ліміт, терміни та умови – це елементи, які можуть змінюватись залежно від банку та продукту.

У сфері операцій з кредитними картками шахрайство має місце, коли кредитор обдурює позичальника, пропонуючи йому покупку, сподіваючись, що рахунок кредитної картки позичальника забезпечить сплату цієї покупки.

В ідеальному випадку сплата не буде здійснена. Якщо ж вона відбудеться, емітент кредитних карток оголосить сплачувану суму. На сьогодні саме через Інтернет відбувається половина випадків шахрайства з кредитними картками. Як правило, шахраї мають зв'язки з певним бізнесом. В області кредитних карток це може бути внутрішня компанія, але найчастіше це зовнішнє підприємство. Стосовно зовнішньої компанії, шахрайство здійснюється майбутнім/існуючим клієнтом або майбутнім/існуючим постачальником. По відношенню до зовнішніх шахраїв можна визначити три різні профілі: звичайний правопорушник, кримінальний злочинець і ті, що входять до злочинних організацій (Фуа та ін., 2005).

Звичайні правопорушники схильні до випадкової та/або нерегулярної нечесної поведінки, тобто коли трапляється нагода, раптова спокуса, або ж коли вони страждають у фінансовому відношенні. Більш небезпечними зовнішніми шахраями є індивідуальні кримінальні злочинці та особи, що належать до злочинних організацій (професіональні/ досвідчені злочинці), позаяк вони неодноразово маскують свою справжню зовнішність та/або розробляють свій спосіб дій, що має злочинний характер (Фуа та ін., 2006; Фуа та ін., 2004).

Для багатьох компаній, які мають справу з численними зовнішніми сторонами, перевірка вручну ідентичності більшості зовнішніх компаній та операцій коштує неймовірно дорого. Насправді, щоб дослідити кожний підозрілий рух, вони наражаються на прямі накладні витрати. Якщо обсяг цього руху менший, ніж накладні витрати, дослідження не має сенсу, навіть якщо щось здається підозрілим (Чан та ін., 1999; Ошервітз, 2005).

2. Види шахрайства

2.1. Шахрайство, пов'язане з банкрутством. У цьому розділі автори зосереджуються на пов'язаному з банкрутством шахрайстві і радять

використовувати звіти бюро кредитної інформації. Шахрайство банкрутства означає використання кредитної картки у разі її неплатоспроможності. Інакше кажучи, покупці використовують кредитні картки, знаючи, що вони не можуть заплатити за свої покупки. Банк надсилатиме їм письмовий наказ для виплати. Так чи інакше, таких клієнтів викриють, оскільки вони потерпатимуть від власного банкрутства і будуть неспроможні покрити борги. Банк змушений буде покрити збитки сам. Зазвичай, такі втрати від шахрайства не входять до підрахунку збитків від шахрайства, оскільки вони вважаються списаними. Єдиним способом запобігання цьому є проведення попередньої перевірки з бюро кредитної інформації з метою отримання чіткого уявлення про банківську історію клієнтів.

У Німеччині, наприклад, найбільш популярними бюро кредитної інформації є SCHUFA і CEG. SCHUFA пропонує послуги своїм клієнтам протягом усього процесу управління ризиком; 62 мільйони записів зберігаються у базі даних. Бюро кредитної інформації звітують про різні підрозділи, такі як приватні банки, ощадні банки, кооперативні банки, спеціальні кредитні заклади тощо та компанії-емітенти кредитних карток.

Зазвичай, процес відбувається таким чином: банк передає запит до бюро кредитної інформації, який містить всі необхідні для бюро дані. У відповідь кредитне бюро відсилає кредитний звіт для цієї особи, включаючи особисті подробиці, деталі невідповідності контрактним зобов'язанням, інформацію від державного керівництва тощо. Деякі кредитні бюро спроможні віднайти адресу певної людини, яка переїхала за "невідомою" адресою.

Інформація в кредитних бюро збирається з різних джерел. Банки, компанії з надання споживчих кредитів, кредитні об'єднання, колекторські агенції є лише частиною організацій, які періодично звітують бюро кредитної інформації. Дані також отримуються з державних та федеральних судів стосовно судових рішень, права утримання майна за борги та оголошення про банкрутство. Кредитні бюро використовують треті сторони для збору інформації. Як правило, приватні фінансові компанії та інші звітують таким бюро щомісяця. Розділ публічних записів кредитного звіту містить серйозну інформацію стосовно банкрутства, слухання справи у суді, накладення арешту на гроші боржника, втрати права викупу закладеного майна, права утримання майна за борги тощо. Дані про банкрутство, отримані з федеральних судів, покривають усі 'пункти' закону про банкрутство і деталі стосовно того, чи спростував суд порушення справи про банкрутство та про кількість банкрутств. Дані про слухання справи у суді, втрату права викупу, записи стосовно права утримання майна за борги від державного та федерального судів заносяться до спеціального списку. Результати збору інформації містяться у розділі публічного запису, якщо вони зібрані податковим органом третьої сторони. Сума, зібрана першочерговою компанією з надання кредиту, може також бути поміщена до розділу торгівлі досьє (Томас та ін., 2002). Інформація зберігається у розділі публічних записів кредитного досьє для різних часових проміжків, що залежать від події та бюро кредитної інформації.

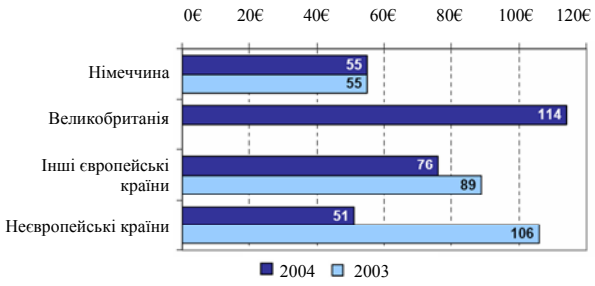
Щойно банк отримав кредитний звіт від бюро кредитної інформації, він має право вирішувати свою політику стосовно відмов. З одного боку, банк може вирішити слідувати консервативному стилю поведінки і обмежити доступ до його продуктів до певного типу клієнта. З іншого боку, він може дозволити собі прийняти високий ризик в плані показників кредитів та шахрайства. Це рішення залежить від виду бізнес-діяльності і портфеля, яким банк хоче управляти. Джерелом критеріїв, що мають значний вплив на виявлення випадків неплатоспроможності, буде збір і судова інформація.

Є кілька інших способів виявлення шахрайства банкрутства. Фостер і Стайн (2004) запропонували модель для передбачення персонального банкрутства серед користувачів кредитних карток. У своїй статті вони описали модель, що базується на методах стандартної регресії. По-перше, модель включала зв'язки та індикаторні функції, необхідні для здобуття нелінійності та відсутніх значень. По-друге, вона базувалась на сучасних теоретичних величинах критеріїв відбору. По-третє, метод, використаний для передбачення стандартної похибки, був досить консервативним, щоб мати справу з залежними одна від одної величинами (Фостер в Стайн, 2004). Об'єднання моделей з метою запобігання банкрутству зі звітами про кредитні операції може бути запропоноване як рішення проти шахрайства банкрутства.

2.2. Шахрайство, пов'язане з крадіжкою/ підробкою. У даному розділі увагу зосереджено на проблемі шахрайства з крадіжками та підробками, які пов'язані одне з одним. Крадіжка означає використання чужої картки. Злочинець викрадає картку і користується нею доти, доки її не заблокують. Чим швидше власник відреагує на крадіжку та зв'яжеться з банком, тим швидше банк вживатиме відповідних заходів. Так само, підробка має

місце тоді, коли кредитна картка використовується дистанційно, тобто необхідні лише її деталі. У певний момент можна скопіювати номер чужої картки та коди і використовувати їх через певні веб-сайти, де не потрібний підпис або картка у матеріальному вигляді. Нещодавно Pago, один з провідних провайдерів міжнародної служби платежів, повідомив у своєму звіті (2005), що шахрайство з кредитними картками є зростаючою загрозою для проданих товарів та послуг через Інтернет. Оптові продавці в режимі он-лайн наражаються на ризик, оскільки вони повинні пропонувати своїм клієнтам виплати кредитною карткою. У випадках, коли шахраї використовують викрадені або підроблені дані кредитної картки, продавець втрачає гроші через так звані "відмови власників кредитних карток від раніше проведеної трансакції". Зазначимо, що ці відмови трапляються тоді, коли власники кредитних карток заперечують щомісячні розрахунки кредитною карткою, оскільки вони не несли відповідальність за покупки.

Незважаючи на те, що, згідно зі Звітом Pago (2005), щорічна кількість відмов у європейській торгівлі через Інтернет здається досить низькою (лише 0.83%), аналітики дуже занепокоєні. Частина відмов, наприклад, через підроблені дані кредитних карток, зросла з 4% у 2003 році до більш ніж 7% у 2004. Це може бути пов'язаним із загальним ростом організованого шахрайства з кредитними картками. Цікавим є те, що кількість відмов серед клієнтів з Німеччини (0.31%) набагато нижча, ніж серед інших європейських споживачів.



Джерело: Звіт Pago, 2005 рік.

Рис. 4. Середня вартість операцій у європейських країнах згідно з походженням клієнтів

Як показано на рисунку 4, поведінка клієнта у здійсненні платежу через Інтернет змінилася протягом 2003-2004 рр. З іншого боку, середня ринкова вартість для німецьких споживачів не змінилась, при 55 євро, тоді як середня вартість для решти Європи була нижчою у 2004 році, ніж у 2003, 79 та 89 євро, відповідно. З іншого боку, неєвропейці мають найвищу середню вартість, 106 євро у 2003 році, тоді як це було найнижчим значенням у 2004 – 51 євро; їх наздогнали британські покупці, які виробили середню вартість, що становила 114 євро – найвища у 2004 році. Отже, середня ринкова вартість значно змінилася з 2003 до 2004 року.

Висновок на основі таких статистичних даних може бути наступним: німецькй ринок кредитних карток меншою мірою піддається впливу шахрайства з кредитними картками, ніж решта країн Європи. Однак це можна вважати справою часу. Виявлення такого виду шахрайства є обов'язковим у бізнесі, пов'язаному з кредитними карткми. І хоча це завдання є надзвичайно складним, цей тип шахрайства можна виявити завдяки так званим 'позалімітним' звітам, які містять щоденний перелік клієнтів, що перевищили свій кредитний ліміт. Може бути прийнятий певний ступінь допустимого відхилення. З власниками кредитних карток, занесених до списку, зв'язуються, і якщо вони не реагують, картка блокується.

Шахрайську операцію важко виявити та визначити. Однак операції, пов'язані з великими сумами та з використанням банкомату, є підозрілими і вимагають контактування з клієнтом. Про покупки товарів на більшу суму, ніж зазвичай, також буде повідомлятися клієнту, так само як і про нетипові закордонні структури витрат. Шахрайським операціям, як правило, неможливо запобігти, оскільки вони трапляються за справді короткий проміжок часу. Однак, коли картку ідентифіковано, її блокують.

2.3. Шахрайство з застосуванням. Шахрайство з застосуванням – це коли хтось використовує кредитну картку з помилковою інформацією. Для виявлення такого типу шахрайства необхідне застосування системи шахрайства, що дозволяє визначати підозрілі випадки використання кредитної картки. При виявленні шахрайства із застосуванням слід розрізняти дві різні ситуації: коли має місце застосування картки однією особою з такими самими деталями, так звані двійники, і коли картка використовується різними людьми зі схожими деталями, так звані ідентичні обманщики.

У більшості банків, щоб мати право на кредитну картку, подавач заяви повинен заповнити бланк, у якому всі поля є обов'язковими за винятком соціальної сфери діяльності.

Необхідна інформація включає дані для ідентифікації, про місцезнаходження, конфіденційну та додаткову інформацію. Повторна інформація вимагається з метою ідентифікації:

повне ім'я та дата народження. Подавач заяви має повідомити банк про своє місцезнаходження: адреса, поштовий код, місто та країна. Працівник банку також запитає про контактні деталі, такі як електронна адреса, телефон наземної лінії зв'язку та мобільний телефон. Конфіденційною інформацією буде пароль. Крім того, надається інформація про стать. Всі ці характеристики будуть використані під час пошуку двійників.

Щоб виявити так званих *двійників*, використовуються перехресні методики. Наприклад, простими питаннями, які дають швидкі результати, є перехресні питання про деталі місцезнаходження: "прізвище, дата народження, поштовий індекс і адреса" або "прізвище, адреса, електронна пошта та стать". За цими питаннями визначаються особи з більш ніж однією карткою. Питання є досить спрощеними, але вони допоможуть усунути із системи більшість двійників. Зазначимо, що двійники, зазвичай, можуть бути справжніми клієнтами, які не мають злочинних намірів. Вони можуть знову звертатися із заявою, вказуючи нову адресу або роблячи інший запис в одному з полів. Натомість, злочин з персональними даними, як його називають, здійснюється справжніми злочинцями, що вносять неправильні дані навмисно.

Фуа та ін. (2006) пояснюють, що шахрайство застосуванням, втілення *злочинності з персональними даними*, трапляється тоді, коли бланки для заявки містять правдоподібну і синтетичну (шахрайство з персональними даними) або справжню, але викрадену інформацію ідентичності (викрадення персональних даних). Згідно з результатами аналізу ID (2004), а також на основі 300 мільйонів фальсифікованих заявок на відкриття рахунку, 88% цих заявок були відкриті з використанням методів викрадення персональних даних. Також, згідно з результатами цього самого дослідження, шахрайство з персональними даними впливає на три чверті загальних втрат, спричинених злочинністю з персональними даними.

Сумісність спрацьовує за умови, якщо хтось мав вдалий досвід здійснення шахрайства. У такому випадку злочинець намагатиметься повторити це з іншим позичальником; таким чином, сумісність може виявити злочинність з персональними даними. Отже, деякі позичальники почали надсилати деталі заявок до центральної бази даних банку, де для виявлення загальних ознак використовуються деякі алгоритми сумісності. Буде застосовуватись багато правил сумісності, і, таким чином, може бути виявлено багато помилкових позитивних випадків (Томас та ін., 2004). Фуа та ін. (2006) запропонували використання методик сумісності, які допомагають виявити численні підозрілі оцінки кредитних заявок.

Рішення: для покращення попарного методу сумісності автори поєднали попарне сумісництво та підозрілу поведінку. Іншим критерієм є кількість активних карток, що відповідають комбінації полів. Метою є визначення важливих полів. Розробка парного сумісництва для динамічних заявок має бути ефективною та дієвою (Фуа та ін., 2006). У справі кредитних карток одним з головних елементів є адреса, тобто куди буде відправлятися картка. Єдиний спосіб для шахраїв отримати декілька карток – це зібрати їх за однією чи кількома адресами. Якщо картки надсилаються за різними адресами під різними іменами, виявлення шахрайства заявки є досить складним. Такі шахраї будуть виявлені пізніше, під час використання картки та поводження згідно з їх резюме (стосовно ліміту, операцій в режимі офлайн, нетипових операцій, статусу невиплати рахунку тощо).

Пропозиція, яка була опротестована, – це попарне згрупування кількості заявок, адрес, поштового індексу та кількості активних карток. При здійсненні правильного попарного поєднання першим кроком є "чистка" заявок. Наприклад, розглянемо німецьку адресу; система має бути розроблена у такий спосіб, що "Hauptstr.29" буде об'єднана попарно з "Hauptstrasse29" або "Heidestrasse85" буде об'єднана попарно з "Heidestr.85". Другий код є подібним до поштового коду; "77756" можна об'єднати з "D-77756". Така попередня робота стосовно даних є дуже важливою для запобігання шахрайським заявкам. Шахраї завжди намагатимуться знайти нові шляхи, щоб зламати систему, тому контрольні чеки мають поновлюватись якомога частіше.

Ми пропонуємо три рівні ризику по відношенню до різної шахрайської поведінки. Рівень 1: "високий ризик " – ця група складається з усіх осіб з однаковою адресою та поштовим індексом та принаймні однією активною карткою, зареєстрованою 10 або більше разів. Рівень 2: "середній ризик " – група складається з усіх осіб з однаковою адресою та поштовим індексом і принаймні однією активною карткою, зареєстрованою щонайменше 5 разів, але менше, ніж 10 разів. Рівень 3: "низький ризик " – група складається з усіх осіб з однаковою адресою і поштовим індексом і щонайменше однією активною карткою, зареєстрованою щонайменше двічі, але менше, ніж 5 разів.

Методи (області застосування): метод був застосований по відношенню до повного набору прикладних даних, що забезпечуються німецьким банком у 2006 році. З метою збереження таємниці банківських операцій нижче представлено лише підрахунок отриманих результатів. Після застосування цього методу список І рівня містить декілька випадків з високою імовірністю шахрайства. Всі згадані особи у цьому списку мали закриті картки. Ситуація є більш складною для іншого списку. ІІ рівень все ще досить обмежений. Посадові особи у справах питання кредиту та інкасації вважали, що половину випадків у цьому списку можна вважати підозрілою та шахрайською поведінкою. Стосовно останнього списку, який є найбільшим, робота є доволі важкою. Менш ніж третина таких клієнтів є підозрілими. Щоб збільшити часову ефективність і накладні витрати, до питання слід включити новий елемент: перші п'ять цифр телефонних номерів, електронна адреса і пароль. Такі питання можуть бути застосовані по відношенню до списку 2 та списку 3.

Ця система не забезпечить 100%-го рішення, але є першим кроком контролю шахрайства з заявкою. Професійні шахраї, звичайно, не будуть виявлені завдяки таким методам, але непрофесіонали – так. Іншим альтернативним рішенням є веб-служба для виявлення кредитної картки, заснованої на співпраці різних банків (Чіу та Тсаі, 2004; Фан, 2004). Ці банки діляться своєю інформацією про шахраїв. Така ідея є цікавою, але важкою для виконання, оскільки вона вимагає співпраці різних банків, які можуть бути не готові поділитися інформацією через конкуренцію на ринку, а також з правових причин.

2.4. Поведінковий обман. Поведінковий обман має місце тоді, коли деталі справжніх карток були отримані шляхом обману, а продажі здійснюються за умови присутності власника картки. Ці продажі включають телефонні продажі та операції купівлі-продажу через Інтернет, де необхідні лише деталі картки (Болтон і Ханд, 2002). Поведінковий обман може бути виявлений завдяки застосуванню фальсифікованої скорингової картки, яка передбачає клієнтів, щоі мають схильність до невиплати.

Традиційні кредитні скорингові картки використовуються для виявлення схильності клієнтів до невиплати (Болтон і Ханд, 2002). Використання скорингу для запобігання обману є подібним до будь-якого іншого застосування, включаючи прибуток, невиплату та інкасацію. Оцінка відображає досвід минулих випадків, а висновком є подвійний результат: справжній клієнт або обманщик.

Головна відмінність полягає в тому, що заявки про професійних обманщиків можуть виглядати, як справжні. Отже, ефективність деяких скорингових заходів для запобігання обману не була доведена, оскільки вони не спроможні розрізняти справжні та фальсифіковані заяви. З іншого боку, якщо використовувати оцінку як перевірку фальсифікації на додаток до використання іншої скорингової моделі як перевірку кредитного ризику, будь-яке удосконалення буде цінним (Томас та ін., 2004). Виявлення власників фальсифікованих заявок є можливим тоді, коли останні пройшли через систему і були клієнтами банку протягом певного часу. Щоб створити скорингову картку, слід визначити короткий біографічний нарис клієнта-обманщика, а також частоту використання картки, види куплених товарів, види операцій, профайли продавців у роздріб, використання готівкових грошей, балансові та платіжні історії, закордонні структури витрат та щоденні, щотижневі, місячні та сезонні структури (Томас та ін., 2004; Сіддікі, 2006).

Із фальсифікованою заявкою обманщики будуть виявлені лише після відсилання рахунків або коли дата сплати почне минати. Затримка в часі є головною проблемою у випадку підозрілих скорингових карток. Загалом, банку знадобиться рік, щоб зібрати достатню кількість важливих даних для побудови цієї моделі та приведення її в дію (Томас та ін., 2002).

3. Способи виявлення

3.1. Дерево рішень. На основі дерева рішень було розроблено ідею дерева схожості, яка визначається рекурсивно: вузлові події позначені приписуваними іменами. Перевагою запропонованого методу є те, що його легко застосувати, зрозуміти і показати. Однак недолік системи полягає у необхідності перевіряти кожну операцію одна за одною.

3.2. Генетичні та інші алгоритми. Алгоритми часто рекомендуються як передбачуваний спосіб виявлення фальсифікації. В основному цей метод слідує скоринговому процесу. В експерименті, що описується у роботі Бентлі та ін. (2000), база даних складалася із 4,000 операцій з 62 полями. Стосовно дерева схожості були застосовані тренувальні і пробні зразки. Цей метод довів результати для справжніх даних страхування життя і може бути ефективним у виявленні шахрайства з кредитною карткою.

Чан та ін. (1999) також розробили алгоритм для передбачення підозрілої поведінки. Оригінальність їх дослідження полягає в тому, що модель оцінюється і підраховується на основі моделі

витрат, тоді як інші автори використовують оцінку, базовану на попередньому розрахунку/ справжньому попередньому розрахунку і помилковому розрахунку/помилковому негативному розрахунку. Вілер та Аіткен (2000) висунули ідею поєднання алгоритмів, щоб збільшити силу прогнозування. У своїй статті вони пропонують різні алгоритми: діагностичні алгоритми, стратегії діагностичних рішень, алгоритми кривої вірогідності, алгоритми найкращої узгодженості, алгоритми негативного вибору та алгоритми вибору щільності. Автори зробили висновок, що базовані на сусідстві та вірогіднісні алгоритми показали себе як непідходящі методи класифікації, які повинні бути покращені шляхом використання додаткових діагностичних алгоритмів для прийняття рішень у випадку стику двох секторів та для обчислення довіри і критеріїв відносного ризику.

3.3. Прийоми групування. Болтон та Хенд (2002) пропонують два прийоми групування шахрайства. Дослідження за групами аналогічних компаній є системою, яка дозволяє виявити рахунки, що поводяться не так, як інші в один момент часу, тоді як вони поводились так само до цього. Ці рахунки потім відмічаються як підозрілі. Дослідники повинні ретельно аналізувати такі випадки. Гіпотеза дослідження за групами аналогічних компаній є наступною: якщо рахунки поводяться однаково упродовж певного періоду, а потім один рахунок поводиться зовсім по-іншому, він обов'язково має бути зареєстрований. Аналіз переривання (Break-point analysis) використовує інший підхід. Гіпотеза наступна: якщо зміна використання картки зареєстрована на індивідуальній основі, цей рахунок повинен бути досліджений. Інакше кажучи, базуючись на трансакціях однієї картки, аналіз переривання може виявити підозрілу поведінку. Сигнали про підозрілу поведінку – це раптова операція на велику суму та висока частота використання.

Таблиця 1. Короткий виклад досліджень, у яких проаналізовано різні статистичні прийоми в області шахрайства з кредитними картками

Дослідження	Країна	Метод	Деталі
Алескеров та ін. (1997)	Німеччина	Нейронні мережі	Система нагляду за картками (card-watch)
Бентлі та ін. (2000)	Великобританія	Генетичне програмування	Логічні правила та процес класифікації (оцінювання)
Болтон та Хенд (2002)	Великобританія	Прийоми групування	Дослідження за групами аналогічних компаній (peer group analysis) та аналіз переривання (break point analysis)
Браус та ін. (1999a)	Німеччина	Методи аналізу даних та нейронні мережі	Використання аналізу даних, який об'єднує вірогіднісний та нейроадаптивний підходи
Чен та ін. (1999)	США	Алгоритми	Прогнозування підозрілої поведінки
Дорронсоро та ін. (1997)	Іспанія	Нейронні мережі	Нейронний класифікатор
Езава та Нортон (1996)	США	Байєсові мережі	Телекомунікаційний сектор
Фен та ін. (2001)	США	Дерево рішень	Індуктивне дерево рішень
Гош та Рейлі (1994)	США	Нейронні мережі	FDS (система виявлення шахрайства)
Кім та Кім (2002)	Корея	Нейронний класифікатор	Покращення ефективності виявлення та зосередження на стандартній похибці перевірної вибірки як у несиметричному розподілі, щоб уникнути помилок у виявленні.
Коккінакі (1997)	Кіпр	Дерево рішень	Ідея дерева сумісності на основі дерева прийняття рішень
Леонард (1995)	Канада	Експертна система	Базована на правилах експертна система для виявлення шахрайства (моделювання шахрайства)
Маес та ін. (2002)	США	Байєсові мережі та нейронні мережі	Індустрія кредитних карток, сигнали про зворотне розповсюдження похибки
Куа та Сріганеш (2007)	Сінгапур	Нейронні мережі	Самоорганізована карта (Self-Organizing Map (SOM)) через систему виявлення шахрайства у реальному часі
Вілер та Айткен (2000)	Великобританія	Поєднання алгоритмів	Діагностичні алгоритми; стратегії діагностичних рішень; алгоритми кривої вірогідності; алгоритми найкращої узгодженості; алгоритми негативного вибору; алгоритми вибору щільності
Заславський та Стрижак (2006)	Україна	Нейронні мережі	SOM (самоорганізована карта), алгоритм для виявлення шахрайських операцій у платіжних системах

3.4. Нейронні мережі. Нейронні мережі є також часто рекомендованим методом виявлення шахрайства. Дорронсоро та ін. (1997) розробили технічно доступну онлайн-систему виявлення шахрайства, базовану на нейронному класифікаторі. Проте головним її недоліком є те, що дані повинні бути згруповані за типом рахунку. Подібними концепціями є наступні: система нагляду за картками card watch (Алексеров та ін., 1997); сигнали про зворотне розповсюдження похибки (Маес та ін., 2002); FDS (система виявлення шахрайства) (Гош та Рейлі, 1994); самоорганізована карта (SOM) (Куа та Сріганеш, 2008; Заславський та Стрижак, 2006); покращення ефективності виявлення (Кім та Кім, 2002). Методи збору та аналізу даних,

такі як ‘Клементина’, уможливлюють використання технологій нейронних мереж, які стали застосовуватись у сфері шахрайства з кредитними картками (Браузе та ін., 1999a; Браузе та ін., 1999b).

Байєсові мережі – ще один метод, який використовується для виявлення шахрайства у телекомунікаційному секторі (Езава та Нортон, 1996) та в індустрії кредитних карток (Маес та ін., 2002). Результати цього методу оптимістичні, однак обмеження в часі є одним з його головних недоліків, особливо у порівнянні з нейронними мережами (Маес та ін., 2002).

Проте, незалежно від того, який статистичний метод обрано, система виявлення шахрайства повинна задовольняти певним умовам. Позаяк кількість шахрайських трансакцій є набагато меншою, ніж загальна кількість операцій, система повинна буде мати справу з несиметричним розподілом даних. У протилежному випадку дані повинні бути розбиті на тренувальні вибірки, де розподіл є менш скошеним (Чен та ін., 1997). Ця система має бути точною з класифікаторами фактичного оцінювання та здатною працювати з викривленнями в даних; запропоноване рішення – очистити дані (Фосетт та Провост, 1997). Ця система повинна бути здатною маніпулювати з частковим перекриттям; шахрайські трансакції можуть бути подібними до звичайних операцій. Оскільки шахраї постійно створюють нові методи, система повинна бути адаптивною та регулярно оцінюватись. Аналіз витрат та прибутків (cost profit analysis) є також необхідним у виявленні шахрайства, щоб уникнути витрачання часу на неекономічні випадки.

У випадку нових емісійних банків пропозиція може базуватись на показниках кредитних бюро, щоб контролювати шахрайство та уникнути передбачених витрат. Хоча ці оціночні карти використовуються здебільшого, щоб “передбачити” клієнтів, які не виконують зобов’язань, хтось може використати їх, щоб виявити шахрайство, оскільки шахрайство та невиконання зобов’язань тісно пов’язані між собою. Основні системи оцінок, як правило, базуються на вибірці з минулого досвіду кількох кредиторів. Основні системи продаються кредиторам, які вірять, що вони є корисними. Ці системи часто є доступними як у випадку трансакцій, так і у випадку покупки (Томас та ін., 2004).

Найбільш переважаючими моделями є ті, які доступні через головні кредитні бюро та впливають на найважливіші кредитні рішення, прийняті основними кредиторами. Показники кредитних бюро можуть бути включені до кредитних звітів індивідуума або як самостійний продукт. Кожне бюро має власні моделі, а конкуренція є напруженою. Хоча у розробці моделі використовується лише інформація з єдиного кредитного бюро, розміри вибірок, як правило, коливаються від сотень тисяч до понад мільйона файлів. Загалом, прогнозуюча здатність загальних моделей бюро є ефективною та подібною до прогнозуючої здатності спеціальних моделей.

В цілому, система показників кредитних бюро розробляється як модель прогнозування “платіжної поведінки” отримувача кредиту. Як правило, показники кредитних бюро базуються на зовнішніх даних, які перевірені у такий спосіб, що, по відношенню до віку та статі, наприклад, вони відображають популяцію (населення). Система показників також встановлюється зі змінними, такими як показник ризику, соціальний та сімейний статус, тип будинку та поштовий індекс.

Для цього компанія Fair Isaac, наприклад, виробляє програмне забезпечення для виявлення шахрайства з кредитними картками. Їхнє рішення базується на методі нейронних мереж, які обробляють трансакційні дані, дані про власника картки та дані про торговельну точку, щоб уникнути шахрайської діяльності. Компанія Experian також розробила власне рішення під назвою Hunter. Pago fraud – ще один інструмент, який використовується для попередження шахрайства. Але оскільки він є занадто дорогим, банки часто не можуть його собі дозволити.

Етичною проблемою, яка випливає з використання методів виявлення шахраїв та “чистих” клієнтів, є те, що можна визначити деяких клієнтів як чесних, коли ті насправді є шахраями, і навпаки, підозрювати у шахрайстві справжніх клієнтів. Ці помилки повинні бути мінімізовані. Проте з точки зору власне банку витрати на визначення клієнта як чесного клієнта, який насправді є шахраєм, є набагато вищими, ніж витрати у випадку, коли чесна людина підозрюється як шахрай. В останньому випадку банк втрачає шанс отримати можливі вигоди. Проте у першому випадку він втрачає капітальну вартість. Щоб працювати на благо акціонерів, банк повинен мати за мету мінімізацію витрат на неправильну класифікацію, а не мінімізацію схильності до неправильної класифікації клієнтів на чесних людей та шахраїв.

Висновок

Однозначно, шахрайство з кредитними картками – це акт кримінально-правового обману. У даній статті оглянуто останні результати досліджень питання шахрайства у сфері кредитних карток. Виявлено різні типи шахрайства, а саме шахрайство банкрутства, махінації з підробленими документами, приховування та знищення офіційних документів, витрачання коштів, поведінкове шахрайство, та обговорено заходи по їх виявленню. Такі заходи включають двоточкову відповідність, дерево рішень, прийоми групування, нейронні мережі та генетичні алгоритми.

З точки зору етики, можна стверджувати, що банки та компанії, які спеціалізуються на випуску кредитних карток, повинні намагатись виявляти всі випадки шахрайства. Однак непрофесійний шахрай навряд чи працюватиме у масштабі професійного злочинця і, таким чином, витрати для банку по їх виявленню можуть стати неекономічними. Банк може зіткнутися з етичною дилемою. Чи повинен він намагатись виявляти такі випадки шахрайства або ж має діяти в інтересах акціонера та уникати неекономічних витрат?

У якості наступного кроку цього дослідження наголос буде на впровадженні 'підозрілої' системи показників та її оцінки. Головними завданнями будуть побудова моделей аналізу для передбачення шахрайської поведінки, беручи до уваги сфери поведінки, що стосуються різних типів шахрайства з кредитними картками, визначеними у цій статті, та оцінка етичного значення. У плані є взяти одну з європейських країн, можливо, це буде Німеччина, а потім розширити дослідження до інших держав-членів ЄС.

Список використаних джерел

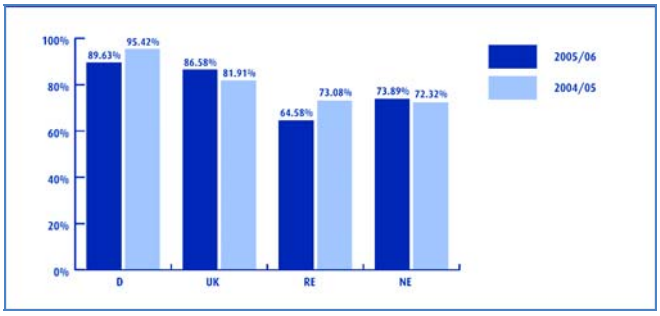
1. Aleskerov, E., Freisleben, B. & B Rao. 1997. 'CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection', Proc. of the IEEE/IAFE on *Computational Intelligence for Financial Engineering*, 220-226.
2. Anderson, R. 2007. *The Credit Scoring Toolkit: theory and practice for retail credit risk management and decision automation*. New York: Oxford University Press.
3. APACS, Association for Payment Cleaning Services, no date. Card Fraud Facts and Figures Available at: http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html (Accessed: December 2007).
4. Bellis, M. no date. Who Invented Credit Cards-the History of Credit Cards? Available at: http://inventors.about.com/od/cstartinventions/a/credit_cards.htm (Accessed: October 2008).
5. Bentley, P., Kim, J., Jung. G. & J Choi. 2000. Fuzzy Darwinian Detection of Credit Card Fraud, Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society.
6. Bolton, R. & Hand, D. 2002. 'Statistical Fraud Detection: A Review'. *Statistical Science*, 17; 235-249.
7. Bolton, R. & Hand, D. 2001. Unsupervised Profiling Methods for Fraud Detection, Credit Scoring and Credit Control VII.
8. Brause R., Langsdorf T. & M Hepp. 1999a. Credit card fraud detection by adaptive neural data mining, Internal Report 7/99 (J. W. Goethe-University, Computer Science Department, Frankfurt, Germany).
9. Brause, R., Langsdorf, T. & M Hepp. 1999b. Neural Data Mining for Credit Card Fraud Detection, Proc. of 11th IEEE International Conference on Tools with Artificial Intelligence.
10. Caminer, B. 1985. 'Credit card Fraud: The Neglected Crime'. *The Journal of Criminal Law and Criminology*, 76; 746-763.
11. Chan, P., Fan, W. Prodromidis, A. & S Stolfo. 1999. 'Distributed Data Mining in Credit Card Fraud Detection'. *IEEE Intelligent Systems*, 14; 67-74.
12. Chan, P., Stolfo, S., Fan, D., Lee, W. & A Prodromidis. 1997. Credit card fraud detection using meta learning: Issues and initial results, Working notes of AAAI Workshop on AI Approaches to Fraud Detection and Risk Management.
13. Chepaitis, E. 1997. 'Information Ethics Across Information Cultures'. *Business Ethics: A European Review*, 6: 4, 195-199.
14. Chiu, C. & Tsai, C. 2004. A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Proc. of 2004 IEEE International Conference on e-Technology, e-Commerce and e- Service.
15. Clarke, M. 1994. 'Fraud and the Politics of Morality'. *Business Ethics: A European Review*, 3: 2, 117-122.
16. Dorronsoro, J. Ginel, F. Sanchez, C. & C Cruz. 1997. 'Neural Fraud Detection in Credit Card Operations'. *IEEE Transactions on Neural Networks*, 8; 827-834.
17. Encyclopedia Britannica, no date. Credit Card. Available at: http://www.britannica.com/eb/article-9026818/credit-card (Accessed: October 2008).
18. Euromonitor International, 2006. Financial cards in Germany Available at: http://www.euromonitor.com/Financial_Cards_in_Germany (Accessed: November 2006).
19. European e-Business Market Watch. 2005. ICT Security, e-Invoicing and e-Payment Activities in European Enterprises, Special Report, September.
20. Ezawa, K. & Norton, S. 1996. 'Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts'. *IEEE Expert*, October; 45-51.
21. Fan, W. 2004. Systematic Data Selection to Mine Concept-Drifting Data Streams, Proc. of SIGKDD04; 128-137.

22. Fan, W., Miller, M., Stolfo, S., Lee, W. & P Chan. 2001. Using Artificial Anomalies to Detect Unknown and Known Network Intrusions, Proc. of ICDM01; 123-248.
23. Fawcett, T. & Provost, F. 1997. 'Adaptive Fraud Detection'. *Data Mining and Knowledge Discovery*, 1; 3.
24. Foster, D. & Stine, R., 2004. 'Variable Selection in Data Mining: Building a Predictive Model for Bankruptcy'. *Journal of American Statistical Association*, 99; 303-313.
25. George, E. 1992. 'Ethics in Banking'. *Business Ethics: A European Review*, 1:3, 162-171.
26. Ghosh, S. & Reilly, D. 1994. 'redit Card Fraud Detection with a Neural-Network, Proc. of 27th Hawaii International Conference on Systems Science, 3; 621-630.
27. Gichure, C. 2000. 'Fraud and the African Renaissance'. *Business Ethics: A European Review*, 9:4, 236-247.
28. ID Analytics. 2004. Identity 2004: The Identity Risk Management Conference.
29. Kim, M. & Kim, T. 2002. A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection, Proc. Of IDEAL 2002, 378-383.
30. Kokkinaki, A. 1997. On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling, Proc. of IEEE Knowledge and Data Engineering Exchange Workshop; 107-113.
31. Leonard K. 1995. 'The development of a rule based expert system model for fraud alert in consumer credit'. *European Journal of Operational Research,* 80; 350-356.
32. Maes, S., Tuyls, K., Vanschoenwinkel, B. & B Manderick. 2002. Credit Card Fraud Detection using Bayesian and Neural Networks, Proc. of the 1st International NAISO Congress on Neuro Fuzzy Technologies.
33. Molyneaux, D. 2007. 'Two case study scenarios in banking: a commentary on *The Hutton Prize for Professional Ethics*, 2004 and 2005'. *Business Ethics: A European Review*, 16:4, 372-386.
34. Oscherwitz, T. 2005. Synthetic Identity Fraud: Unseen Identity Challenge, Bank Security News, 3; 7.
35. Pago-Report. 2005. The development of E-commerce sectors, ©Pago eTransaction Services GmbH.
36. Pago-Report. 2007. Trends in Consumer Purchasing and Payment Behaviour in selected E-commerce Industries, ©Pago eTransaction Services GmbH.
37. Phua, C., Alahakoon, D., & V Lee. 2004. 'Minority Report in Fraud Detection: Classification of Skewed Data'. *ACM SIGKDD Explorations: Special Issue on Imbalanced Data Sets*, 6; 50-59.
38. Phua, C., Gayler, R., Lee, V., & K Smith. 2006. On the Approximate Communal Fraud Scoring of Credit Applications, *Proceedings of Credit Scoring and Credit Control IX.*
39. Phua, C., Lee, V., Smith, K. and Gayler, R., 2005. A Comprehensive Survey of Data Mining-based Fraud Detection Research., Artificial Intelligence Review.
40. Quah T. S, & Sriganesh M. 2008. 'Real-time credit card fraud using computational intelligence'. *Expert Systems with Application*, 35:4, 1721-1732.
41. Siddiqi, N. 2006. *Credit Risk Scorecards: Developing And Implementing Intelligent Credit Scoring*, John Wiley & Sons, USA.
42. Thomas, L.C., Edelman, D.B., & J.N Crook. 2002. *Credit Scoring and its Applications*, SIAM Monographs on Mathematical Modeling and Computation, Philadelphia.
43. Thomas, L.C., Edelman, D.B., & J.N Crook. 2004. *Readings in Credit Scoring: Foundations, Developments, and Aims*, Oxford University Press, USA.
44. Wheeler, R. & Aitken, S. 2000. 'Multiple Algorithms for Fraud Detection'. *Knowledge-Based Systems*, 13; 93-99.
45. Zaslavsky V. & Strizhak A. 2006. 'Credit card fraud detection using self-organizing maps'. *Information and Security*, 18; 48-63.

Отримано 28.05.2009
Переклад з англ. Філатової Ю.

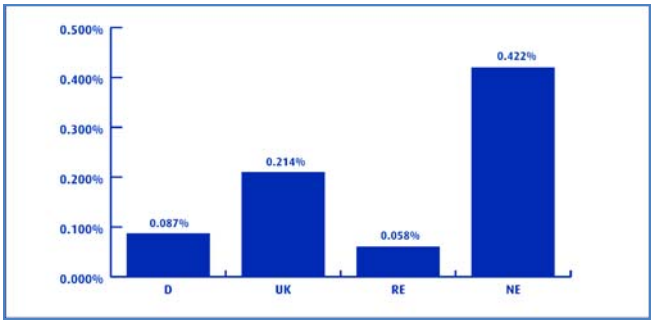
Додаток А. Коефіцієнти результативності та норми повернення платежів

Як показано на рисунку А.1, коефіцієнти результативності значно погіршились у Німеччині (D) і залишились на тому ж рівні для клієнтів з решти країн Європи (RE), за винятком показників для клієнтів з Великобританії та неєвропейських країн (NE), які є вищими, ніж раніше. Коефіцієнти результативності для власників кредитних карток з решти країн Європи є меншими, ніж 65%*.



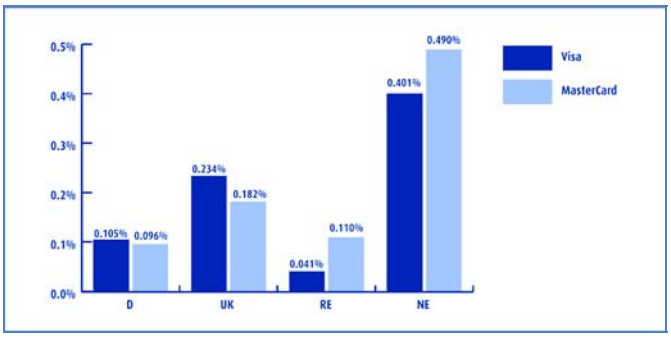
Джерело: Pago e-Transaction Services GmbH, Звіт Паго, 2007.

Рис. А.1. Коефіцієнти результативності для операцій з кредитними картками, здійснюваними клієнтами у всіх магазинах (за країною клієнта)



Джерело: Pago e-Transaction Services GmbH, Звіт Паго, 2007.

Рис. А.2. Норми повернення платежів для операцій з кредитними картками, здійснюваними клієнтами у всіх магазинах (за країною клієнта)



Джерело: Pago e-Transaction Services GmbH, Звіт Паго, 2007.

Рис. А.3. Норми повернення платежів для операцій з кредитними картками у всіх магазинах (за маркою кредитної картки та країною клієнта)

Як показано на рисунку А.2, середній коефіцієнт повернення платежів становить близько 0.33%. Цей показник для трансакцій з німецькими клієнтами є вражаюче низьким – 0.087%. Так само, він є низьким для клієнтів у решті країн Європи, 0.058%. Для клієнтів-неєвропейців та британців ці коефіцієнти становлять 0.422% та 0.214%, відповідно. Для неєвропейців норма повернення платежів впала, проте вона залишається найвищою серед усіх груп. Слід наголосити на тому, що ця ситуація відрізняється від тієї, що мала місце в 2004 році, коли жодна з груп клієнтів не мала коефіцієнта повернення платежів, який би був нижчим за 0.10%. У якості висновку можна сказати наступне, ризик невиплати вже не є проблемою для електронних комерційних операцій.

Ризик невиплати та бренд кредитної картки змінюються залежно від різних груп, як показано на рисунку А.3. Для користувачів з Німеччини та решти Європи цілком зрозуміло, що коефіцієнти Visa та MasterCard є досить низькими порівняно з такими самими показниками для користувачів поза межами Європи та навіть для клієнтів з Великобританії.

* Це найгірший показник, який коли-небудь був представлений у Звіті Паго.