Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Detekce bankovních podvodů pomocí SQL

Kateřina Nekorancová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Kateřina Nekorancová

Informatika

Název práce

Detekce bankovních podvodů pomocí SQL

Název anglicky

Banking Crime Detection using SQL

Cíle práce

Cílem práce analýza bankovních podvodů a způsoby jejich detekce a prevence. Dále bude práce obsahovat popis relačních databází a jejich využití k odhalování nelegální činnosti. Práce bude zakončena návrhem vlastního scénáře detekce.

Metodika

Použije standardy softwarového inženýrství, jako např. UML, metody návrhu relačních databází (normalizace, dekompozice, syntéza) a ANSI/ISO SQL standardy.

Doporučený rozsah práce

30-40 stran

Klíčová slova

bankovní podvody, relační databáze

Doporučené zdroje informací

ANTUŠÁK, E. – KOPECKÝ, Z. – VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. KATEDRA MANAGEMENTU. SEKCE KRIZOVÉHO MANAGEMENTU. *Krizový management : krizová komunikace.* Praha: Oeconomica, 2005. ISBN 80-245-0945-8.

JAMES, L. – Phishing bez záhad. Praha: Grada Publishing, 2007. ISBN 978-80-247-1766-1

LACKO, Ľ. *SQL : hotová řešení : pro SQL Server, Oracle a MySQL.* Brno: Computer Press, 2003. ISBN 80-7226-975-5.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

doc. Ing. Vojtěch Merunka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 20. 2. 2016

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 20. 2. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 04. 03. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Detekce bankovních podvodů pomocí SQL" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2016 Kateřina Nekorancová

Poděkování

Děkuji vedoucímu bakalářské práce doc. Ing. Vojtěchu Merunkovi, Ph.D. za cenné rady, připomínky a metodické vedení práce.

Detekce bankovních podvodů pomocí SQL

Souhrn

Tato bakalářská práce na téma „Detekce bankovních podvodů pomocí SQL“ se v teoretické části zaměřuje na seznámení s databázemi. Stručně popisuje vývoj databází, způsob uložení dat v databázích dle definovaných pravidel, vzájemné vztahy mezi tabulkami a proces normalizace. Dále obsahuje přiblížení podvodů v bankovnictví, jejich rozdělení, nástroje napomáhající k jejich odhalování a následné prevenci jejich opětování s využitím databázových systémů.

Praktická část obsahuje návrh možného scénáře podvodu využívající poznatky z praktické části. Obsahuje vzorové tabulky s údaji o klientech, podaných žádostech a zaměstnavatelích, které klienti udávají do žádostí, a tabulku blacklist k ověřování společností. Tabulky jsou spojeny pomocí klíčů a navrženým příkazem jsou z tabulek vybírány podezřelé společnosti. Za podezřelé považujeme ty, u kterých roste množství podaných žádostí za určité období. Tyto společnosti jsou pak prověřeny v tabulce blacklist.

Klíčová slova:

databáze, SŘBD, SQL, bankovní kriminalita, podvody, detekce a prevence, analýza, nástroje detekce, blacklist

Banking Crime Detection using SQL

Summary

This bachelor thesis on „Banking Crime Detection using SQL“ focuses in theoretical part on approach to databases. It describes progression of database, methods of storing data in databases according to defined rules, interrelationships between tables and normalization process. It contains approach to bank fraud, distribution of fraud, instruments to assist the detection of fraud and follow prevention of iteration whit the use of database systems.

Practical part contains proposal possible screenplay fraud uses knowledge of theoretical part. It contains sample tables containig data about clients, filed application and employers, which clients indicated in the application, and blacklist table to authentication company. Tables are linked through keys and suspicionus company are selected from tables. Company is regarded as suspicionus if it grows at the amount of application submitted. That company is verified in table blacklist.

Keywords:

database, DBMS, banking crime, fraud, detection and prevention, resources of detection, black list

Obsah

1 Úvod

Nárůst podvodů v bankovním sektoru má mnoho příčin. Zejména konkurenční boje o potenciální klienty znamenají pro banku nastavit dostupnější podmínky k získání finančních prostředků. To vytváří příležitost pro pachatele podvodů. Rozvoj techniky a vznik internetového bankovnictví je příčinou nárůstu počítačových podvodů, kdy terčem útoků jsou klienti i banky samotné. Objevují se stále nové metody a technologie útoků, proto musí být banka o krok napřed a orientovat se v technikách podvodů, aby jim mohla co nejdříve čelit.

Banky jsou dnes vybaveny obsáhlými databázemi disponujícími kolem miliardy záznamů o klientech. Správné využití těchto informací nám umožňuje analyzovat a vyhodnotit údaje získané od klientů. Pro banky je velmi důležité spravovat vlastní databázi a také informace sdílet s ostatními institucemi.

Tato bakalářská práce se v teoretické části snaží přiblížit základní znalosti ohledně databází. Následuje rozbor nejčastěji vyskytujících se podvodů v bankovnictví a rozbor problematiky detekce a prevence podvodů.

Praktická část využívá poznatků z teoretické části, kdy aplikujeme techniku detekce, tzv. Early Fraud Detection, k odhalení určité podvodné činnosti. Pomocí vytvořeného schématu podvodu vybíráme z databáze podezřelé společnosti. Zaměřuje se na organizované zločiny, kdy je společnost založena za účelem pozdějšího získávání finančních prostředků od bankovních ústavů tím, že na pobočce banky žádá o úvěr fiktivní zaměstnanec této společnosti.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je analýza bankovních podvodů a způsoby jejich detekce a prevence. Dále práce obsahuje popis relačních databází a jejich využití k odhalování nelegální činnosti. Práce je zakončena návrhem scénáře podvodů.

2.2 Metodika

K sepsání práce byly použity standardy softwarového inženýrství, jako například UML, metody návrhu relačních databází (normalizace, dekompozice, syntéza) a ANSI/ISO SQL standardy.

3 Databáze

Databáze, jinak také datová základna, je systém souborů s pevnou strukturou záznamů. Jsou tvořeny jednou nebo více tabulkami, které jsou navzájem propojeny. Slouží k ukládání dat a jejich následné zpracování. Data mezi sebou mají určité vztahy a jsou určitým způsobem členěna. V širším pojetí spadají do pojmu databáze i softwarové prostředky, které umožňují manipulaci s uloženými daty a přístup k nim. Jejich pomocí můžeme data editovat, vyhledávat, rovnávat nebo třídit. Tento software je označován jako systém řízení báze dat (SŘBD).

Výhodou využití databáze oproti uložení dat do souboru je takový, že databáze obvykle fungují mnohem rychleji. Umožňují nám data vypisovat, řadit a propojovat, a to pomocí skriptu. Navíc bývají optimalizovány pro přístup více uživatelů a obsahují mechanismy usnadňující práci s daty.

3.1 Historie

Jako předchůdce databáze se označuje papírová kartotéka. Umožňovala uspořádání dat dle určitých kategorií a následné zatřiďování nových položek. Všechny operace s kartotékou probíhaly manuálně. Zpracovávání dat se začalo převádět na elektromechanické stroje, paměťovým médiem byl v tomto případě děrný štítek. Velkým impulzem pro další vývoj databází byl vývoj počítačů. Původní používání strojového kódu procesorů se ukázalo jako neefektivní, objevil se požadavek na univerzální databázový jazyk. Výsledkem byla první verze jazyka COBOL pro hromadné zpracování dat. Později se začala vytvářet koncepce databázových systémů, vznikaly první síťové SŘBD na sálových počítačích. Začínaly se objevovat pojmy jako schéma databáze, jazyk pro definici schématu, subschéma a podobně. Ve stejné době byly vyvíjeni hierarchické databáze. Jeden z prvních SŘBD byl IMS, který stále patří k nejrozšířenějším na sálových počítačích. S tím souvisí i vývoj prvních relačních databází, pohlížejících na data jako na tabulky, a první verze jazyka SQL. Tento vývoj přinesl výkonově použitelné systémy, srovnatelné se síťovými a hierarchickými databázemi. Poté se začínaly objevovat objektově orientované databáze a vznikla objektově-relační technologie.

3.2 Systém řízení báze dat

Systém řízen báze dat (zkráceně SŘBD nebo DBMS) je označení pro softwarové vybavení, které zajišťuje práci s databází, tzn. tvoří rozhraní mezi aplikačními programy a uloženými daty. Jeho úkolem je efektivní zpracování velkého množství dat, musí být schopen data ukládat, modifikovat, mazat a provádět dotazy. SŘBD je nedílnou součástí velké většiny aplikací, zejména pak podnikových s více vrstvou architekturou. „Úloha DBMS stoupá s velikostí databáze, počtem uživatelů a distribucí databází v různých lokalitách (typické pro velké nadnárodní organizace a internetové portály).“ [1]

3.3 RDBMS

„DBMS pro relační databáze se označuje jako RDBMS (Relational Database Management System). Jedná se o program nebo sadu programů, které data uchovávají, spravují načítají, mění a manipulují s nimi v jedné nebo více relačních databázích. Příkladem takového programu je například DB2 od společnosti IBM nebo sharewarový produkt MySQL. Tyto programy, stejně jako jiné RDBMS, umožňují pracovat s daty uloženými v jejich systémech. Ačkoli sytém RDBMS nemusí být založen na SQL, většina produktů na trhu na něm založena je a snaží se o dodržení jeho standardu.“[2]

3.4 Databázové modely

Během let bylo implementováno mnoho modelů databází pro ukládání a správu dat. Z hlediska způsobu ukládání dat a vazeb mezi nimi můžeme rozdělit databáze do základních typů:

3.4.1 Hierarchické databáze

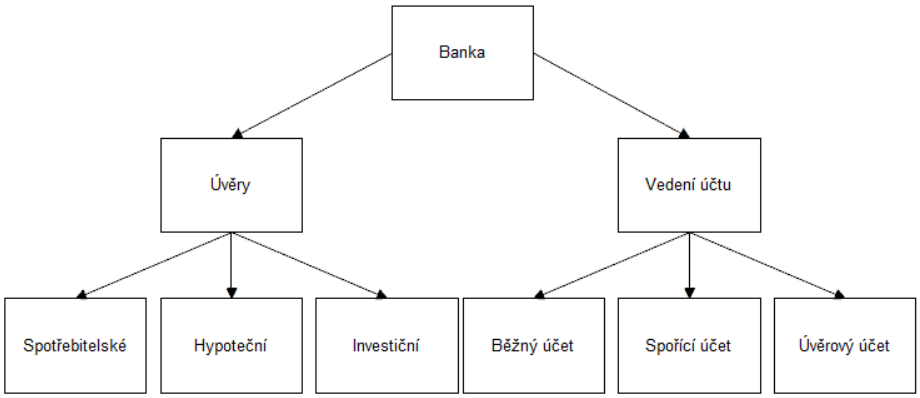
Tento model má víceúrovňovou strukturu, která je podobná obrácenému stromu. Nadřazené tabulce může náležet mnoho podřízených tabulek, ale podřízená tabulka má

[1] Oppel, A. Databáze bez předchozích znalostí. 2006. s. 12

[2] Kroenke, David a Auer, David. Databáze. místo neznámé : Computer Press, 2015. s. 28

vždy jen jednu nadřazenou. Hierarchická databáze byla využívána zejména v době ukládání dat na magnetické pásky, zvláště proto, že přístup k datům byl pouze sekvenční. Dnes je model často považován z důvodu jeho neflexibilní struktury a nedostatečné podpory složitých vztahů pro mnoho aplikací za nevhodný. Mnoho implementací však obsahuje funkce, které obchází tato omezení.

Obrázek 1 Příklad hierarchické databáze

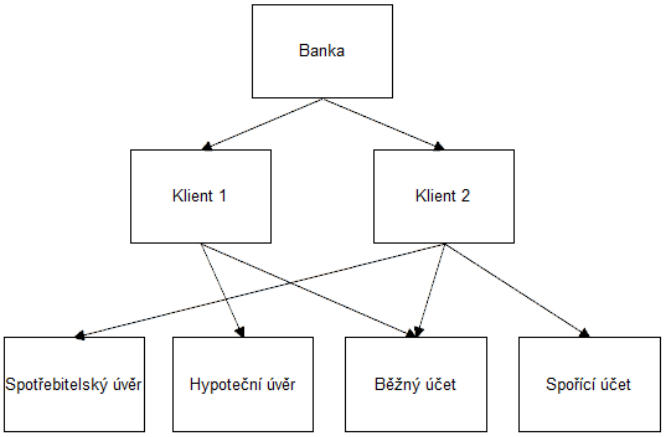


Zdroj: http://www.databaze.chytrak.cz/modely.htm

3.4.2 Síťové databáze

Síťový model hledá uspokojivá východiska z některých omezení hierarchického modelu. Struktura je zde podobná, ale tabulky jsou organizovány do skupin, jež vztahují dvojice tabulek k vlastníkům a členům. Jakákoliv tabulka může být součástí jakékoliv skupiny s ostatními tabulkami v databázi, která podporuje složitější dotazy, než jaké podporuje hierarchický model. Síťový model má však také svá omezení. Pro práci se skupinami musíme velmi dobře znát databázi a je obtížné měnit strukturu bez vlivu na aplikace, které s databází spolupracují.

Obrázek 2 Příklad síťové databáze



Zdroj: http://www.databaze.chytrak.cz/modely.htm

3.4.3 Relační databáze

Relační databáze řeší mnohá omezení hierarchického a síťového modelu. V těchto modelech aplikace spoléhá na nadefinovanou implementaci databáze, jež je pak napevno začleněna do aplikace. Při přidání nového atributu do databáze je třeba úprava aplikace, a to i v případě, že tento atribut nepoužívá. Relační databáze je na aplikaci nezávislá, lze měnit strukturu bez vlivu na aplikaci. Struktura relační databáze je založena na relaci nebo tabulce, což umožňuje definování složitých vztahů mezi těmito relacemi. Každá relace může být považována za samostatnou entitu bez různých omezení definice vztahů mezi tabulkami. Relační model nahradil mnoho systémů využívající hierarchické či síťové databáze a je nejčastěji implementovaným modelem v moderních databázích. Právě relační model je základem pro SQL.

Obrázek 3 Příklad relační databáze

ID	příjmení	jméno	r_číslo
0001	Novák	Jan	780915/5214
0002	Dvořák	Karel	651204/1841
0003	Straka	Josef	890128/3941

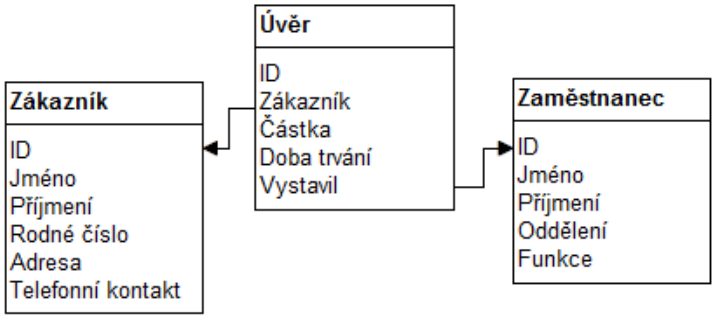
r_číslo	č_účtu	pobočka
780915/5214	2548467	Palackého
651204/1841	5847296	28.října
890128/3941	5748699	Moskevská

Zdroj: http://www.databaze.chytrak.cz/modely.htm

3.4.4 Objektové databáze

Objektově orientovaná databáze je systém správy databází, ve kterém je informace představena formou objektů stejně jako v objektově orientovaných programovacích jazycích. „Pro objektové databáze neexistuje žádný oficiální standard, dá se za něj považovat kniha Morgana Kaufmana The Object Database Standard: ODMG – V2.0.“[3] Výhodou tohoto systému je snadnější přístup a podpora versioningu. Využívá se v oblastech s velkými počty dat o jednom předmětu, a to například v bankovnictví pro práci s rozsáhlými daty jako je třeba výpis transakcí. Daní využití je dále v inženýrství, telekomunikaci, fyzice částic nebo molekulární biologii.

Obrázek 4 Příklad objektové databáze



Zdroj: http://www.databaze.chytrak.cz/modely.htm

3.4.5 Objektově relační databáze

Tento model se snaží sjednotit rysy jak relačních, tak objektových databází. Trvalé informace zůstávají v tabulkách, ale některé položky mohou mít bohatší datovou strukturu, nazývanou ADT, neboli Abstraktní Datové Typy. Tyto typy vznikají kombinací základních datových typů. Operace a funkce asociované s novými datovými typy mohou být použity k indexování, ukládání a získávání záznamů na základě obsahu nového datového typu.

[3] Veselá, Judita. Relační databáze jako nástroj pro analýzu a prezentaci dat. 2014. s. 15

3.5 Databázová integrita

„Integrita je stav, při němž data uložená v databázi vyhovují soustavě určitých definovaných pravidel.“[4] Do databáze tedy lze zadávat pouze data, která vyhovují těmto pravidlům. Pravidla se obvykle vztahují na rozsah uložených hodnot, respektování datového typu nastaveného pro daný sloupec tabulky, nebo na vazby mezi uloženými záznamy.

3.5.1 Integritní omezení

K zajištění integrity slouží integritní omezení. To zahrnuje nástroje, které zabrání vložení nesprávných dat či ztrátě nebo poškození stávajících záznamů v průběhu práce s databází. Například je možné zajistit mazání dat, která již ztratila svůj význam; například pokud smažeme uživatele z databáze, odstraní se i zbytek jeho záznamů v ostatních databázových tabulkách.

Entitní integritní omezení

Zajišťuje, aby o jedné entitě nebylo možno do databáze vložit duplicitní záznamy. Jde tedy o zajištění unikátnosti skutečných identifikátorů reálných objektů.

Doménové integritní omezení

Zajišťuje dodržování datových typů definovaných u sloupců databázové tabulky.

Referenční integritní omezení

Zabývají se vztahy dvou tabulek, kde jejich relace je určena vazbou primárního a cizího klíče.

Aktivní referenční integrita

Definuje činnost, které databázový systém proveden, pokud jsou porušena některá pravidla.

[4] Kroenke, David a Auer, David. Databáze. Computer Press, 2015. s. 34

3.6 Relační databáze

Relační databází rozumíme databázi založenou na relačním modelu. Často tento pojem označuje nejen databázi samotnou, ale i její konkrétní softwarové řešení. V tabulkách relačních databází řádky obvykle představují záznamy a eventuálně některé sloupce v nich chápeme tak, že uchovávají informace o relacích mezi jednotlivými záznamy. Dle relační teorie lze pomocí základních operací (sjednocení, spojení, projekce, selekce, rozdíl a kartézský součin) uskutečnit veškeré operace s daty, ostatní operace jsou již jen kombinací těchto základních.

3.6.1 Relace

„Relace, neboli databázové tabulky, jsou základním konstruktorem relačních databází. Jsou to dvourozměrné struktury tvořené záhlavím a tělem. Řádky se nazývají záznamy, sloupce představují atributy. Atributy mají určen svůj konkrétní datový typ a doménu, což je množina přípustných hodnot daného atributu. Řádek je řezem přes sloupce tabulky a slouží k vlastnímu uložení dat.“[5]

3.6.2 Primární klíč

Primární klíč je jednoznačný identifikátor záznamu, řádku tabulky. Primárním klíčem může být sloupec nebo kombinace více sloupců, ovšem tak, aby byla zaručena jeho jednoznačnost. Pole primárního klíče musí obsahovat nějakou hodnotu, tzn. nesmí obsahovat prázdnou hodnotu NULL. Lze použít i umělý klíč, což je číselný nebo písmenný identifikátor. Nové záznamy jsou opatřeny odlišnými identifikátory od všech předešlých záznamů. Obvykle se používají celočíselné řady; každý novější záznam dostává číslo o jednotku vyšší než je číslo u posledního vloženého záznamu.

[5] Conolly, T: Mistrovství - Databáze: Profesionální průvodce tvorbou efektivních databází. 2009. s. 26

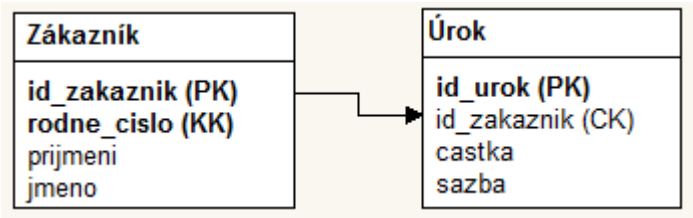
3.6.3 Kandidátní klíč

Kandidátní klíč, nebo také klíč kandidáta je atribut, popřípadě skupina atributů, který jednoznačně identifikuje záznam v relační tabulce. Kandidátní klíč se může stát primárním. Ostatní, které se primárním klíčem nestanou, jsou označovány jako alternativní.

3.6.4 Cizí klíč

Cizí, nebo také nevlastní klíč, slouží k vyjádření vztahů mezi tabulkami. Jedná se o pole či skupinu polí, která umožní identifikovat souvislost mezi záznamy z různých tabulek.

Obrázek 5 Primární klíč, cizí klíč a klíč kandidáta



Zdroj: http://www.dotnetportal.cz/clanek/60/Lehky-uvod-teorie-databazi

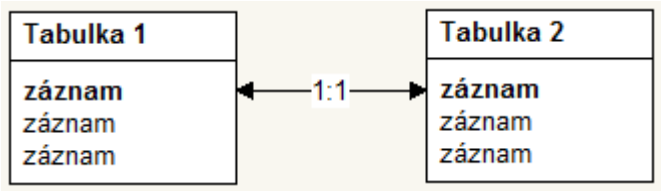
3.7 Druhy vazeb

Vazby definují vzájemná propojení mezi tabulkami navzájem. Tato propojení nám pomáhají zamezit zadání nesprávných hodnost, umožňují rychlejší práci s vyplňování hodnot a nabízejí možnost třídění záznamů v dotazech. Hlavní výhodou je, že pokud změníme údaj v jedné tabulce, údaj se opraví i druhé tabulce, se kterou je spojena. Definujeme tři druhy vazeb:

Vazba 1:1

Jedné položce z první tabulky náleží jedna položka v tabulce druhé, například klienti a rodná čísla, kdy každému klientovi náleží právě jedno rodné číslo. Tyto vazby se vyskytují velmi zřídka, většinou se jedná o chybné navržení databáze.

Obrázek 6 Vazba 1:1

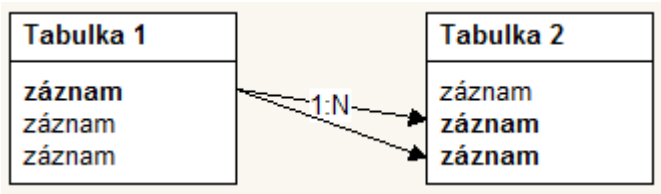


Zdroj: http://gml.vse.cz/data/oppa-webdesign/zaklady-db.html

Vazba 1:N

Jedné položce z první tabulky náleží několik položek z druhé tabulky. Příkladem takovéto vazby může být například banka a její klienti, tedy jedné bance náleží více klientů. Tato vazba je nejpoužívanější zejména při tvorbě rozsáhlých databází.

Obrázek 7 Vazba 1:N

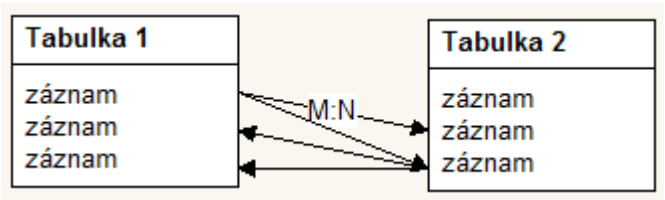


Zdroj: http://gml.vse.cz/data/oppa-webdesign/zaklady-db.html

Vazba M:N

Několika položkám z jedné tabulky náleží několik položek jiné tabulky, například klient a produkty, kdy klient může využívat více produktů a naopak určité produkty může využívat více klientů. Abychom mohli v databázi s touto vazbou pracovat, je třeba ji převést na vazbu 1:N pomocí spojovací tabulky.

Obrázek 8 Vazba M:N



Zdroj: http://gml.vse.cz/data/oppa-webdesign/zaklady-db.html

3.8 Normalizace

„Normalizace je označení pro postup přeorganizování struktury dat za účelem minimalizace počtu redudantních dat, zjednodušení práce s daty a jejich lepší manipulace. Správné navržení struktury hodnotíme pomocí normálních forem, což jsou určitá pravidla, která by data v relaci měla splňovat.“[6] Každá vyšší forma nám více zjednodušuje práci s daty, vyšší formy v sobě zahrnují formy nižší.

Nultá normální forma (0NF)

Relace je v nulté normální formě, pokud v ní existuje pole obsahující více hodnot. Máme například tabulku bankovních institucí s atributy ID, název, datum založení a poskytované služby. Ve sloupci poskytované služby se vyskytuje více hodnot. Řešením je rozdělení atributu na více sloupců.

První normální forma (1NF)

Relace je v první normální forma, pokud její atribut obsahují pouze atomické hodnoty, tedy z pohledu databáze je již nelze dále dělit. Například v relaci s informacemi o klientech máme více telefonních čísel k jednotlivým osobám. S takovouto tabulkou by se špatně pracovalo. Aby tabulka vyhovovala normě, rozdělíme atribut telefonní číslo do více atributů nebo vytvoříme samostatnou tabulku pouze pro telefonní čísla, což je podstatně flexibilnější řešení.

Druhá normální forma (2NF)

Relace je v druhé normální formě, pokud je v první normální formě a každý atribut je plně závislý na celém primárním klíči. Tuto formu tedy využíváme, pokud máme v tabulce vícehodnotový primární klíč. Například máme tabulku s informacemi o zaměstnancích s atributy ID, oddělení a nadřízený. Klíčem této tabulky je kombinace atributů ID a oddělení. Řešením je opět rozdělení na dvě tabulky.

[6] Lacko, Ľ. SQL: hotová řešení pro SQL Server, Oracle a MySQL. Brno : Computer Press, 2003. s. 31

Třetí normální forma (3NF)

V třetí normální formě je relace, která splňuje předchozí formy a neexistuje závislost mezi neklíčovými atributy. Příkladem může být tabulka s produkty banky. Primárním klíčem je zde ID produktu, dále tabulka obsahuje atributy název, oddělení zabývající se tímto produktem a kontakt na toto oddělení. Všechny atributy jsou závislé na primárním klíči, avšak oddělení a kontakt jsou závislé mezi sebou. Řešením je taktéž rozdělení na více tabulek.

Boyce-Coddova normální forma (BCNF)

Boyce-Coddova normální forma je variace třetí normální formy, je i vymezena stejnými pravidly. BCNF nám říká, že mezi kandidátními klíči nesmí být funkční závislost. Platí klasické řešení rozložení na více tabulek.

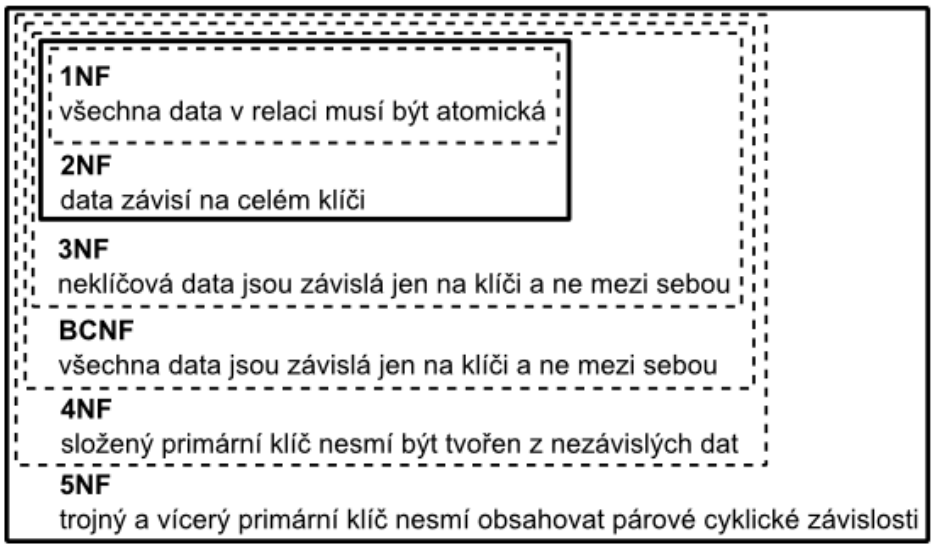
Čtvrtá normální forma (4NF)

Relace je ve čtvrté normální formě, je-li v BCNF a pokud její atributy popisují pouze příčinnou souvislost, tedy jeden fakt. 4NF se zabývá vztahy uvnitř složeného primárního klíče. U tabulek se složeným primárním klíčem se může stát, že některé hodnoty tohoto klíče na sobě budou nezávislé. Je třeba, aby klíč tvořily hodnoty, které mají skutečnou vzájemnou souvislost.

Pátá normální forma (5NF)

Relace je v páté normální formě, pokud je ve čtvrté a zároveň do ní nelze přidat další atribut, jehož vlivem by se poté rozpadla na více relací. Forma se zabývá redudancí dat a možnou ztrátou závislosti.

Obrázek 9 Normální formy



Zdroj: http://gml.vse.cz/data/oppa-webdesign/zaklady-db.html

4 SQL

SQL (Structured Query Language) je strukturovaný dotazovací jazyk používaný pro práci s daty v relačních databázích. Je založeno na relačním modelu, ačkoli není jeho přesnou implementací. Relační model poskytuje teoretické základy relační databáze, zatímco SQL podporuje fyzickou implementaci. SQL je téměř univerzálně implementovaný relační jazyk. Jako neprocedurální jazyk se zabývá více výsledky operací, než jejich samotnou definicí. Základní softwarové prostředí určuje, jak budou operace zpracovány. Nedá se ovšem říci, že by SQL nepodporovalo procedurální funkce. Například uložené procedury, součástí standardu SQL:1999, umožňují procedurální zpracovaní.

SQL je často označováno jako podjazyk, stále mu chybí mnoho základních prvků většiny jiných počítačových jazyků. Nejčastěji je používáno ve spojením s programovacími jazyky aplikací, které nejsou navržené pro manipulaci s daty uloženými v databázi. SQL je tedy používáno v kombinaci s aplikačním jazykem jako efektivní prostředek pro přístup k datům.

4.1 Historie

„Po publikování relačního modelu začala společnosti IBM vyvíjet jazyk a databázový systém pro implementaci tohoto modelu. Ve své definici byl jazyk označován SEQUEL a po pozdější revizi byl přejmenován na SQL. Když společnost IBM vyvíjela relační databázový systém založený na SQL, jiné společnosti začaly vyvíjet své vlastní produkty založené na SQL. Ve skutečnosti společnost Relation Software, Inc., nyní Oracle Corporation, vydala svůj databázový systém ještě před tím, než společnost IBM uvedla svůj produkt na trh. Jak stále více společností vydávalo své produkty, stával se z SQL standardní jazyk pro relační databáze.“[7]

V roce 1986 vydala standardizační supina ANSI první publikovaný standard pro jazyk (SQL-86), aktualizován byl v roce 1989 a znovu v roce 1992. SQL-92 představoval rozsáhlé rozšíření jazyka o některé funkce a vylepšení funkcí oproti předchozím verzím. O sedm let později byla vydána poslední verze standardu SQL, SQL:1999, představující další velký krok kupředu, kterým se SQL přiblížilo skutečným implementacím databázových systémů a potřebám jejich uživatelů.

4.2 Popis jazyka

„SQL příkazy se nejčastěji rozdělují na čtyři základní skupiny podle funkce, kterou provádí;

Jazyk definice dat (DDL - Data Definition Language)

Příkazy DDL se používají k vytváření, upravování nebo odstraňování databázových objektů, tedy tabulek, schémat, domén, pohledů, triggerů a uložených procedur. Klíčovými slovy SQL nejčastěji spojovanými s příkazy DDL jsou CREATE, ALTER a DROP, neboli příkazy pro vytvoření, změnu vlastností nebo odstranění definice objektu.

[7] Molinaro, A. SQL: Kuchařka programátora. 2009. s. 19

Jazyk pro řízení dat (DCL - Data Control Language)

Tyto příkazy umožňují řídit, kdo bude mít přístup k určitým objektům v databázi. Pomocí jazyka DCL můžeme povolovat nebo naopak zamezovat přístup. Slouží k tomu příkazy GRANT nebo REVOKE. Příkazy DCL umožňují řízení typu přístupu každého uživatele k databázovým objektům. Můžeme například určit, kteří uživatelé budou moci určitou skupinu dat pouze prohlížet, a kteří budou moci manipulovat s daty. Do této skupiny lze přiřadí i příkazy pro řízení transakcí; START TRANSACTION, COMMIT a ROLLBACK pro zahájení, potvrzení či zrušení transakce.

Jazyk pro manipulaci s daty (DML - Data Manipulation Language)

Jazyk DML se používá k prohlížení, přidávání, upravování nebo odstraňování dat uložených v databázových objektech. Nejčastěji používané příkazy jsou SELECT, INSERT, UPDATE a DELETE (dále také třeba MERGE, EXPLAIN nebo SHOW). Nejdůležitější příkaz SELECT slouží k načítání dat s tabulky.“[8]

Ostatní nebo speciální příkazy

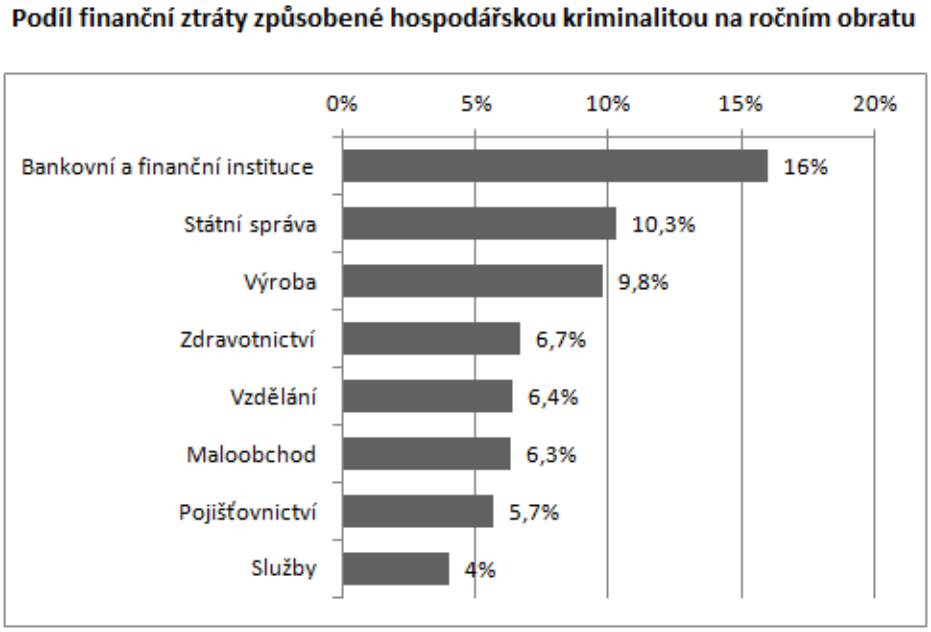
Tyto příkazy slouží ke správě samotné databáze. Umožňují přidávat uživatele nebo nastavovat systémové parametry, tzn. kódování znaků, způsob řazení, formáty data a času, apod. Tyto příkazy nejsou standardizovány a konkrétní syntaxe je závislá na databázovém systému.

[8] Oppel, A. Databáze bez předchozích znalostí. 2006. s. 23

5 Bankovní kriminalita

Bankovní kriminalita se objevila spolu se vznikem prvních bank. S rozvojem bankovnictví vznikají pro zločince nové příležitosti. Podoba podvodů se příliš nemění, změny probíhají zejména v technických prostředcích využívaných pachateli. Naopak v prostředí bank existuje mnoho prostředků k odhalení a následné prevenci podvodů a další stále vznikají.

Graf 1 Ztráty v jednotlivých odvětvích



Zdroj: http://www.aec.cz/index.php?id=585,1050,0,0,1,0

5.1 Podvod

Podvodem se rozumí úmyslné jednání za účelem obohacení na úkor společnosti nebo klienta záměrným zkreslením údajů, neoprávněných využitím služby, zcizením peněz apod.. Ke spáchání podvodu musí existovat příležitost, podnět jednotlivce k podvodnému jednání a také jeho schopnost si odůvodnit motiv k jeho spáchání.

Podvody patří mezi tzv. operační rizika, zabývá se jimi risk management.

5.1.1 Definice dle zákona č. 40/2009 Sb.

„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“[9]

5.2 Důvody spáchání podvodu

Důvody pro spáchání podvodu mohou být různá, nejčastější však bývá chamtivost. Tu pak doprovází potřeba udržení nákladného životního stylu nepodporovaného platem či tlak na dosažení vyššího zisku. Impulsem může být i kariérní zklamání, pocit nespravedlnosti či nedostatečné ohodnocení.

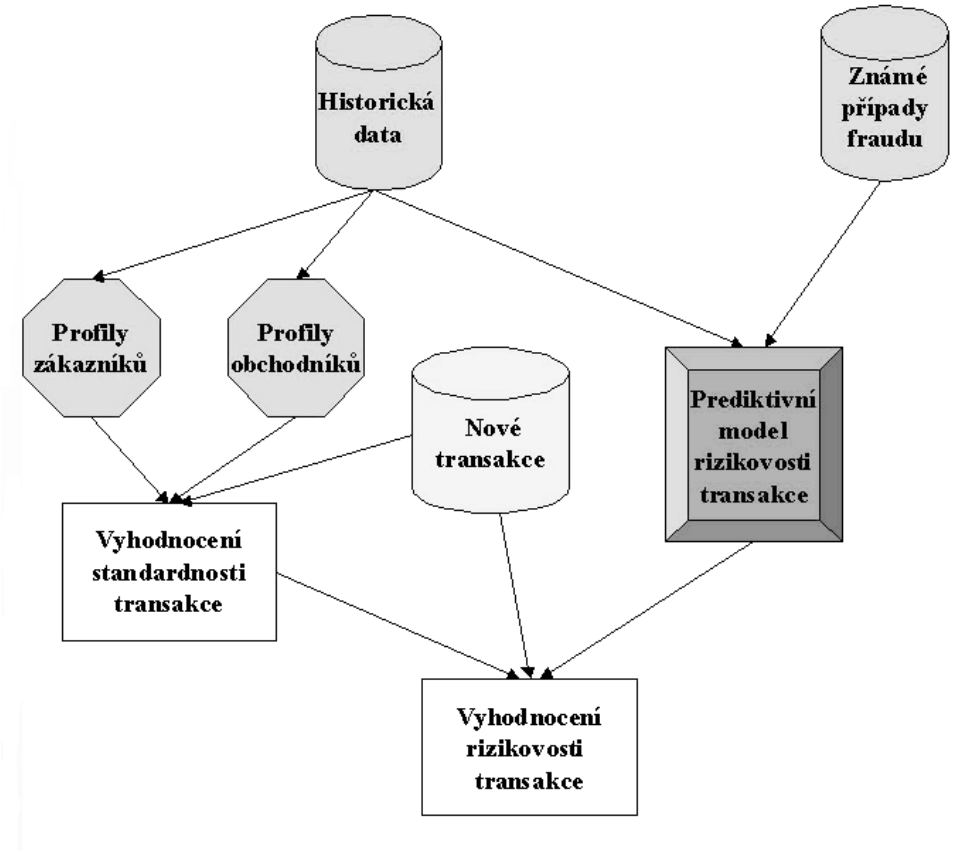
5.3 Řízení rizik v bankovnictví

Tuto činnost má na starost oddělení risk management, který má za úkol identifikovat a kvantifikovat riziko pomocí analýzy a následné implementace patřičných opatření ke snížení rizika. Tomuto oddělení se ve struktuře jednotlivých bank přikládá velká váha, zejména proto, že se mu daří minimalizovat nebezpečí plynoucí z aktivit banky a udržovat vysokou efektivnost. Riziko je úzce spojené s výnosem, pokud tedy banka podcení řízení rizik, může to ovlivnit její ziskovost.

Řízení rizik probíhá pod dohledem ČNB v souladu s pravidly BASEL III, které byly zavedeny 1.ledna 2013. Jde o třetí verzi tzv. Basilejské dohody, která se stala povinností pro všechny tržní subjekty. Cílem těchto pravidel je zejména podpora bezpečnosti a stability finančního sektoru, zohlednění všech rizik a posílení bankovního dohledu a trhu.

[9] Dostupné z: http://business.center.cz/business/pravo/zakony/trestni_zakon/cast2h9.aspx

Obrázek 10 Postup vyhodnocení rizika



Zdroj: http://en.wikipedia.org/wiki/Bank_fraud

5.3.1 Rozdělení rizik

Podstatou rizika je určitá nahodilost, proměnlivost možných výsledků a zejména pak možnost odchylky od předpokládaného vývoje. Dle pragmatického přístupu k riziku jde o hodnotu zachycující potenciální ztrátu.

Úvěrové riziko

„Banka je vystavena riziku, že klient nedostojí svým závazkům dle podmínek smlouvy. Z toho důvodu se prověřuje bonita klienta a využívá prostředků k zajištění minimalizace tohoto rizika, kterými jsou například ručení nebo postoupení pohledávek.“[10] Příčiny úvěrového rizika mohou mít interní charakter, kdy jde o špatný odhad rizika, nebo

[10] Polouček, S. Bankovnictví. 2006. s. 51

externí, které nejsou závislé na bankovní instituci. Může se jednat o celkový vývoj ekonomiky či politickou situaci.

Úrokové riziko

Toto riziko je spojené se změnou tržních úrokových sazeb a jejich dopadu na zisk banky. Pro snížení míry rizika je třeba přizpůsobit strukturu aktiv a pasiv v účetnictví tak, aby měly přibližně shodnou úrokovou citlivost na změny tržních sazeb.

Měnové riziko

Měnové riziko závisí na změnách měnových kurzů. Řešení je obdobné jako u úvěrového rizika, tedy sladění struktury aktiv a pasiv nebo využití termínovaných kontraktů.

Likvidní riziko

Banka by měla být dostatečně likvidní, tzn. schopna dostát svým závazkům. Měla by být tedy schopna vyplatit splatné vklady. K zabezpečení likvidity je třeba vytvářet dostatečné portfolio s přijatelným množstvím likvidních prostředků nebo mít možnost sjednání úvěrových linek s jinými bankami.

Kapitálové riziko

Tržní hodnota závazků by neměla být vyšší než tržní hodnota aktiv. Banka by měla mít k dispozici dostatek vlastního kapitálu k pokrytí ztrát. Tržní hodnota veškerých aktiv by neměla klesnout pod hodnotu závazků.

Operační riziko

Riziko ztrát vzniká v důsledku technických, organizačních či personálních chyb v rámci bankovní instituce. Jde tedy o riziko ztráty vlivem nedostatku či selhání vnitřních procesů, lidského faktoru nebo systémů banky. Předcházet těmto rizikům můžeme například pomocí rekvalifikačních kurzů zaměstnanců.

5.4 Fraud management

Fraud management je útvar zabývající se řízením rizik bankovních podvodů. Využívá počítačové simulace detekčních strategií banky a porovnává je s aktuálně používanými postupy. Kvalitní Fraud management pak dokáže přibližně předpovědět limit možné ztráty způsobenou podvodným jednáním pro určité časové období. Pomocí tzv. backtestingu pak zjišťujeme rozsah výkyvu předpovězené a skutečné ztráty.

Obrázek 11 Fraud Management

Zdroj: http://www.gfo.cz/page.php?show=vzdelani&id=5&PHPSESSID=964332471e26553e61e097e1a11017dd

5.5 Typy podvodů

Podvody lze rozdělit do několika skupin, které charakterizují společné faktory. Faktorem může být postup podvodu, četnost jeho výskytu nebo způsob jeho odhalování.

5.5.1 Aplikační podvody

Prostředkem těchto podvodů jsou falešné či pozměněné doklady totožnosti, popřípadě jiné doklady či písemnosti. Jedná se podvody prováděné na základě krádeže identity. Klient při uzavírání smlouvy předkládá falešné, upravení či kradené doklady totožnosti. Pachatel ovšem může využít zcizené identity i k přístupu k bankovnímu účtu nebo k přístupu

k citlivým informacím. Pro poškozenou osobu není nejhorší samotná krádež informací, ale škody způsobené jejich využitím. „Krádež identity je nejčastějším druhem podvodu v bankovnictví, je tedy důležité jim věnovat největší pozornost.“[11]

Dalším aplikačním podvodem je případ, kdy pachatel v žádosti o poskytnutí úvěru uvádí nepravdivé či zkreslené informace. Například uvádí neexistující kontaktní údaj, na kterém ho nelze kontaktovat, nebo nepravdivou informaci o výši příjmu, zaměstnavateli nebo době trvání pracovního poměru. Dále může zastírat skutečnost zadlužení u jiné instituce či informaci o vztahu k zaměstnanci banky.

Jiné příklady aplikačních podvodů jsou žádosti pro jinou osobu, u nichž klient povětšinou jedná pod nátlakem třetí osoby, nebo klient neplatící své závazky vůči bance.

5.5.2 Transakční podvody

Transakční podvody spočívají v neoprávněném pohybu peněz na bankovních účtech prováděné osobou, jež není majitelem účtu. Může se jednat o osobu předstírající, že je vlastníkem účtu za účelem získat finanční prostředky tohoto účtu. Dalšími případy jsou zfalšování podpisu na příkazu k úhradě nebo transakce s padělanou či ukradenou kartou. Za podvodnou transakci se považuje i provedení platby kartou, která nebyla držitelem autorizována.

5.5.3 Post aplikační podvody

Jde o podvody, kdy podvodné jednání probíhá až po poskytnutí úvěru. Nepravdivé údaje jsou klientem poskytovány při procesu vymáhání peněžních prostředků. Například si klient vytvoří fiktivní obrat díky pravidelným platbám na účtu se záměrem získat co vyšší úvěrový rámec, po dosažení hranice využívá veškeré půjčené prostředky a úvěr přestane splácet. Jiný případ spočívá v nahromadění závazků klienta, kdy si v krátkém časovém intervalu půjčuje finanční prostředky s cílem krytí předchozích úvěrů. Závazky tedy splácí, ale úvěry se hromadí a časem není klient schopný úvěry splácet.

[11] Smejka, V. Řízení rizik ve firmách a jiných organizacích. 2013. s. 42

Do aplikačních podvodů lze také zařadit zpronevěru, kdy si podvodník přivlastní finanční prostředky, které mu nenáleží.

5.5.4 Ostatní podvody

Dalším podvodem se kterým se můžeme setkat, je tzv. praní špinavých peněz (Money laundering), nebo také legalizace výnosů z trestné činnosti. Jde o jednání zastírající původ získaných prostředků z trestné činnosti, tedy navození dojmu, že prostředky byly získány v souladu s platnými zákony. Průběh podvodu spočívá ve vkladu hotovosti na účet, zastření jejich původu a následné vrácení majiteli k investování do legální činnosti.

„V současné době je stále více používána podvodná technika označená jako phishing. Jde o způsob získávání citlivých údajů v elektronické komunikaci. Typickým příkladem je zasílání e-mailových zpráv obsahujících výzvy adresáta k zadání osobních údajů na fiktivní stránku, která je téměř identická s oficiální webovou stránkou banky. Jde například o napodobení přihlašovacího okna internetového bankovnictví.“[12]

5.6 Rozdělení podvodů dle vztahu pachatele k bance

Podvody lze dělit podle toho, zda pachatel operuje v prostředí bank či nikoli, dělíme je tedy na podvody interní a externí.

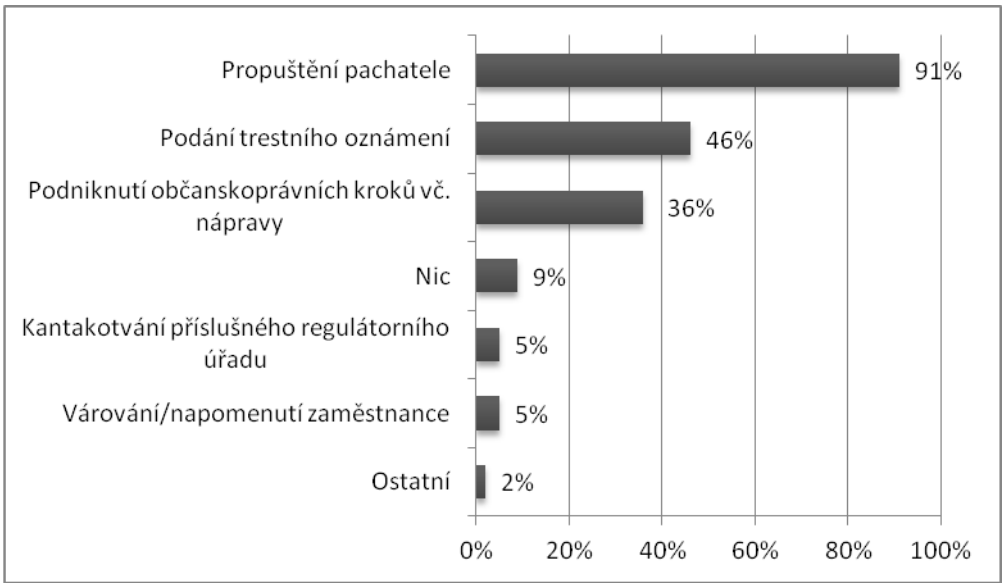
5.6.1 Interní

Tyto podvody jsou velmi nebezpečné zejména z důvodu podrobné znalosti interního prostředí instituce, ať už z hlediska struktury či ochranných mechanismů banky. Pachatel má tedy příležitost k páchání zločinu a k následnému zastření důkazů. Největší příležitost k podvodu vzniká tam, kde zaměstnanec jedná samostatně bez kontroly. Interní podvody se však vyskytují u řídících pracovníků, kteří bezpečnostní standardy sami nastavují. Proto musí fungovat nejen detekce, ale i následné kontroly. Důležitá je práce fraud managementu, která může předem určit, kde může k podvodům dojít.

[12] James, L. Phishing bez záhad. Praha : Grada Publishing, 2007. s. 9

Zaměstnanec například poskytne úvěr společnosti, která krátce po nabytí prostředků vyhlásí bankrot, prodá interní informace osobě zvenčí, vědomě upraví údaje v žádosti nebo neoprávněně převede peníze na svůj osobní účet.

Graf 2 Nápravná opatření vůči pachatelům interních podvodů

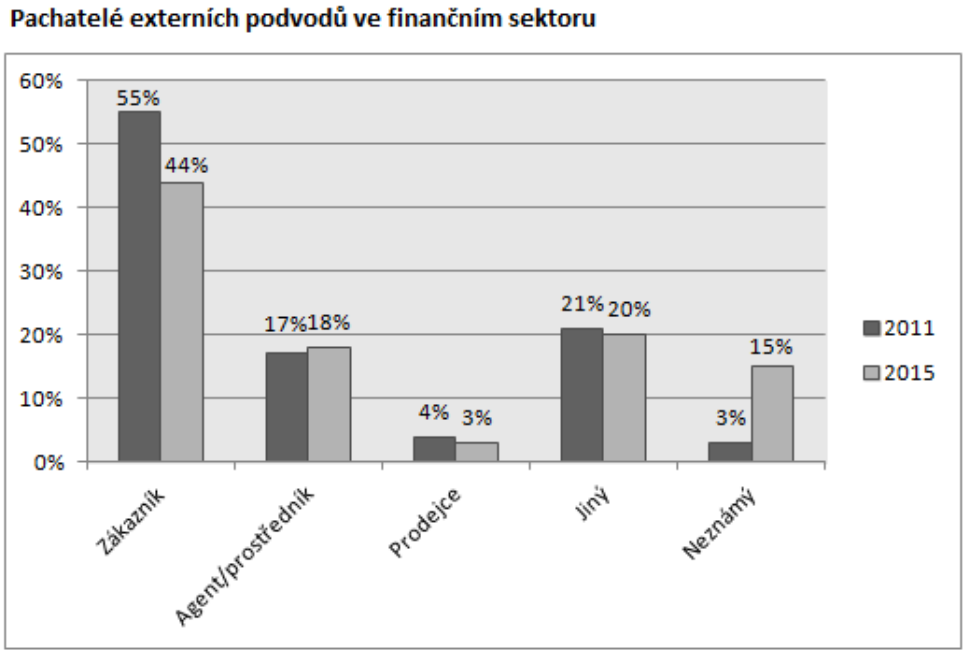


Zdroj: http://www.aec.cz/index.php?id=585,1050,0,0,1,0

5.6.2 Externí podvody

Jedná se o podvody ohrožující bankovní systém zvenčí, kdy pachatel není zaměstnancem banky, nemusí mít k bance žádný vztah, popřípadě se může jednat o zákazníka, dodavatele či poskytovatele služeb banky. Příkladem takovýchto podvodů jsou podvody se šeky, zneužití platební karty nebo zpronevěra.

Graf 3 Pachatelé externích podvodů



Zdroj: http://www.gfo.cz/page.php?show=vzdelani&id=5&PHPSESSID=964332471e26553e61e097e1a11017dd

5.7 Detekce a prevence podvodů

„V současné době je v oblasti bankovnictví alarmující nárůst ztrát zapříčiněný podvodným jednáním klientů. Hlavním důvodem je zejména virtualizace služeb; stále více využívané internetové bankovnictví nebo půjčky online. S vývojem technologií se zdokonalují způsoby překonávaní ochranných mechanismů. Je velmi těžké takovým jednání zabránit, proto je důležitý vývoj a aplikace ochranných prostředků.“[13] Oblasti detekce a prevence spolu úzce souvisí. Je důležité podvod nejen odhalit, ale také zabráni uskutečnění podobnému jednání pomocí opatření, která budou schopna rozpoznat potencionální podvodné jednání dle charakteristických znaků zachycených při předchozích případech. Kromě vlastních záznamů banky využívají i jiných zdrojů, jako například Policii ČR nebo státní zastupitelství.

[13] Smejka, V. Řízení rizik ve firmách a jiných organizacích. 2013. s. 23

Samotná detekce spočívá v prověřování podezřelých osob, a to za pomocí interních aplikací banky a vnějších zdrojů. V případě odhalení podvodu následuje stručná analýza a vložení osoby na tzv. Blacklist. Případ se poté předává týmu Investigace nebo trestnímu oddělní, které na pachatele podává trestní oznámení.

5.7.1 Black list

„Black list (černá listina) bankovních klientů, je interní databáze osob nebo organizací, které se dopustily podvodu. Jsou zde evidovány i osoby neplnící své závazky vůči bance nebo osoby podezřelé z podvodného jednání nebo jiné trestné činnosti. Black list plní dvě základní úlohy, pomáhá identifikovat podezřelé subjekty a zároveň brání těmto subjektům pokračovat v podezřelé aktivitě. To činí pomocí určitých omezení nebo sankcí.“[14] V případě podání žádosti o úvěr osob uvedených na listině je tato žádost ověřována či úplně zamítnutá dle závažnosti jeho provinění. Hlavním důvodem vložení osoby či organizace na black list je zejména podvodné jednání, zneužití identity či padělání dokladů. Při výměně informací mezi registry se nahlíží do úvěrové zprávy klienta, který je o tom informován, a přístup odsouhlasí. Registr spravuje společnost CEDR, a.s., podle které ho využívá celkem 95% bankovního trhu.

5.7.2 Registr dlužníků

V roce 2006 vznikl v České republice spojením Bankovního registru klientských informací (BRKI) a Nebankovního registru klientských informací (NRKI) univerzální registr pro výměnu dat, tvořící největší databázi úvěrových vztahů, tedy nástroj pro posouzení rizika žadatele pro poskytovatele finančních služeb. „Registry obsahují negativní i pozitivní informace o palební morálce a bonitě klientů finančních institucí. Nejedná se tedy o negativní registr poukazující výhradně na dluhy klientů, předkládá i pozitivní platební historii umožňující klientům dosáhnout kvalitní služby i v případě jejich drobných prohřešků.“[15]

[14] Dostupné z: http://www.mesec.cz/clanky/slozite-prani-spinavych-penez/

[15] Dostupné z: https://www.centralniregistrdluzniku.cz/

5.8 Nástroje detekce podvodů

Pro odhalování podvodů v bankovnictví je nejdůležitější kvalitní analýza informací a externích zdrojů využitím specializovaných softwarů. Pomocí analýzy se vytváří určitá typologie podvodů ze známých případů, mapují se nové typy podvodů a následuje studie vnitřních procesů a kontrolních mechanismů banky. Na základě analýzy se navrhují řešení v podobě změn pracovních postupů nebo využívání kontrolních mechanismů.

5.8.1 Sběr a evidence dat

Hlavním zdrojem informací jsou předešlé případy podvodů, především pak jejich provedení. K evidenci podvodného chování klientů nám slouží již zmíněné blacklisty. Získané informace využíváme nejen k detekci budoucích potenciálních podvodů, ale také ke kvantifikaci škod způsobené bankovní instituci, to později poslouží k rozhodování vedení společnosti. Data se zaznamenávají jedině elektronicky, důležitá je strukturovanost dat, s tím spojené dodržování určité metodiky a používání jednoznačných klíčů pro napojení do databází. Významné je především využívání odkazů, to snižuje administrativní zátěž. Důležité je rovněž propojení databází, to nám poslouží k verifikaci dat již při zadávání.

Evidovaná data:

- předmět podvodu; tedy způsobené škody, jejich výše
- osoby odpovědné za škody, zejména pak čísla účtů (žádosti)
- spojení škody a osob
- časové údaje; vznik problému, zjištění podvodu, zahájení analýzy, atd.
- lokace; místo vzniku
- použité prostředky

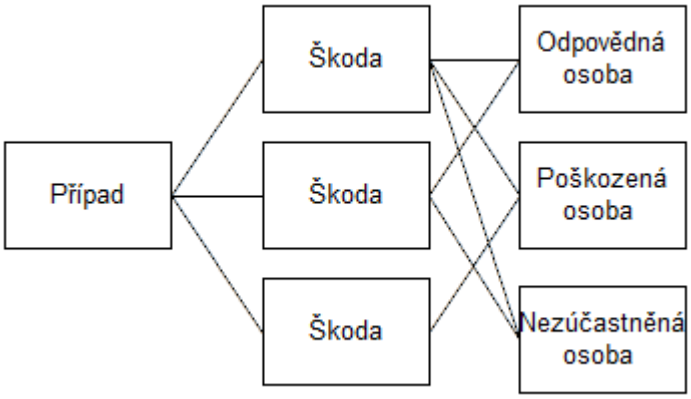
U bankovních produktů je zaznamenaný rozsah škody buď výše úvěrového limitu (počítaného s úroky nebo bez úroků), výše opravných položek, výše zůstatku nebo výše odpisu se započtenými náklady na vymáhání.

Obecně by se mohlo zdát, že by ideálním řešením bylo sbírat co nejvíce informací. Překážkou však můžou být vysoké náklady. Cena by rozhodně neměla přesáhnout případné

škody. Dalším problémem by zde mohla být fragmentace dat, tedy příliš detailní zápisy. Je zbytečné evidovat například data, která se dají jednoduše odvodit z jiných. Případné duplicitě dat se můžeme vyhnout evidováním pouze vazby s databází klientů, v případě klientských dat, nebo s databází produktů u produktových dat. Případy pak lze flexibilně kombinovat pomocí vztahů.

Schéma případných vazeb případů:

Obrázek 12 Schéma vazeb



Zdroj: http://www.aec.cz/index.php?id=585,1050,0,0,1,0

5.8.2 Fraud detection systems

Dalším prostředkem detekce podvodného jednání je Fraud detection systems, nebo také FDS. Jde o označení informačních systémů, které mají na starost jejich bezpečnost, a to nejen ve fázi prevence, ale v celém průběhu životního cyklu události. Tyto systémy se nejčastěji využívají v elektronickém bankovnictví pro případ odcizení přihlašovacích údajů. Dále se využívají v systému bankovních karet nebo v procesu schvalování úvěrů.

Hlavní komponentou celého FDS je Scoringový engine, který vyhodnocuje míru pravděpodobnosti výskytu podvodu pomocí určených metod. Pro využití tohoto systému je nezbytné využití databázi nebo datových skladů s velkým množstvím dat. Výše nároků na databáze se odvíjejí od složitosti používaného enginu. Aplikace systému pak probíhá pomocí modulů pro konkrétní oblasti, například již zmíněné internetové bankovnictví, využitím prostředků databáze a enginu. Případy k detekci pak FDS přijímá pomocí

vstupně/výstupních rozhraní, zpětně pak posílá informace o pravděpodobnosti výskytu podvodu, případně příkazy k provedení určité akce.

Výhodou tohoto systému je zejména zhodnocení uživatelů a jejich aktivit v porovnání s předpokládaným chováním. Systém rovněž umožňuje identifikovat podezřelé události pomocí gelokačních mechanismů.

5.8.3 Fraud Scorecard

Skórekarta (Fraud Scorecard) detekuje podvody na základě údajů uvedených v žádostech klientů. Klienti jsou rozdělováni do různých rizikových skupin podle určitých parametrů (např. rizikovosti segmentu nebo úrokové sazby). Ukazatelé, což jsou jednotlivé položky žádostí, pomáhají ohodnotit bonitu klienta. Pro správné ohodnocení je důležitá úplnost zadávaných údajů, při vynechání některých položek se snižuje kvalita detekce. Ukazatelé jsou většinou odlišné pro různé instituce nebo oblasti, to ztěžuje sdílení dat mezi oblastmi.

Tabulka 1 Fraud Scorecard

Rating	Výsledné skóre	Riziko	Max. částka	Úroková sazba
A	441 a více	minimální	500 000 Kč	9,8%
B	423 - 440	nízké	350 000 Kč	10,5%
C	387 - 422	střední	200 000 Kč	12,5%
D	353 - 386	vysoké	80 000 Kč	14,8%
E	352 a méně	maximální	0 Kč	-

Zdroj:https://www.fiserv.com/customer-channel-management/online-banking/fraud-detection-system.aspx

5.8.4 Skóringové modely

Tyto modely využívají statistické analýzy ke kvantifikaci rizik spojeného s klientskou žádostí o úvěr. Výsledný scoring je v podstatě odhad schopnosti klienta splácet úvěr. Model pracuje s databází současných klientů, kterým byl poskytnut úvěr, s údaji o průběhu splácení. Kromě ohodnocení úvěrového rizika poskytuje i základ pro tvorbu marketingových a vymáhacích strategií.

Příklad hodnocení klienta:

Tabulka 2 Klasifikace dle rizikového faktoru

Rizikový faktor	váha (v %)	klasifikace (1 - nejlepší, 6 nejhorší výsledek)										
		1	1,5	2	2,5	3	3,5	4	4,5	5	5,5	6
platební morálka	28					84						
otázka kreditu	30				75							
podnikatelský rozvoj	6				15							
situace v zakázkách	6							24				
právní forma	10			20								
stáří firmy	8	8										
roční obrat	6	6										
obrat/zaměstnanci	2		3									
základní kapitál	4	4										
celkem	100	18	3	20	90	84	-	24	-	-	-	-
index bonity	239											

Zdroj: https://www.fiserv.com/customer-channel-management/online-banking/fraud-detection-system.aspx

Tabulka 3 Třídy bonity

Třída bonity	Index bonity	pravděpodobnost defaultu na horizontu jednoho roku
1	100 - 149	0,10
2	150 - 200	0,25
3	201 - 250	0,60
4	251 - 300	1,25
5	301 - 350	3,00
6	351 - 499	10,00
7	500	likvidace
8	600	insolvence, úpadek

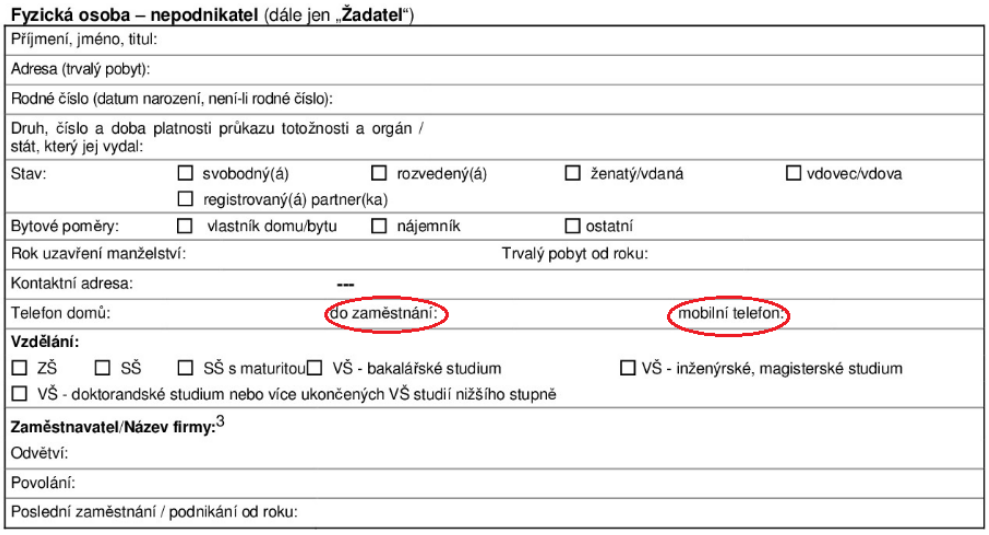
Zdroj: https://www.fiserv.com/customer-channel-management/online-banking/fraud-detection-system.aspx

5.8.5 Verifikační proces

Verifikační proces, nebo také proces autentizace, spočívá v kontaktování klienta telefonní nebo elektronickou cestou. Například ověříme uvedená telefonní čísla v telefonním seznamu či na internetových stránkách firmy. Při telefonickém kontaktování ověřujeme údaje zadané v žádosti; zejména osobní údaje, informace o společnosti a pracovním poměru. Klienta vždy kontaktujeme alespoň na jednom z telefonních čísel uvedených v žádosti. Ověřené údaje musí souhlasit s údaji na žádosti. Pokud jsou ověření

kladná, lze tato telefonní čísla použít k prověření klienta. Při zjištění nesrovnalostí se spojíme s týmem prevence podvodů a udáme podmět k šetření.

Obrázek 13 Žádost o úvěr



Fyzická osoba – nepodnikatel (dále jen „**Žadatel**")

Příjmení, jméno, titul:				
Adresa (trvalý pobyt):				
Rodné číslo (datum narození, není-li rodné číslo):				
Druh, číslo a doba platnosti průkazu totožnosti a orgán / stát, který jej vydal:				
Stav:	☐ svobodný(á)	☐ rozvedený(á)	☐ ženatý/vdaná	☐ vdovec/vdova
	☐ registrovaný(á) partner(ka)			
Bytové poměry:	☐ vlastník domu/bytu	☐ nájemník	☐ ostatní	
Rok uzavření manželství:		Trvalý pobyt od roku:		
Kontaktní adresa:	---			
Telefon domů:	do zaměstnání:		mobilní telefon:	
Vzdělání:				
☐ ZŠ ☐ SŠ ☐ SŠ s maturitou ☐ VŠ - bakalářské studium ☐ VŠ - inženýrské, magisterské studium				
☐ VŠ - doktorandské studium nebo více ukončených VŠ studií nižšího stupně				
Zaměstnavatel/Název firmy:[3]				
Odvětví:				
Povolání:				
Poslední zaměstnání / podnikání od roku:				

Zdroj: http://www.uvery-pujcky-hypoteky.cz/Allianz-www.Allianz.cz/

5.8.6 Fraud monitoring

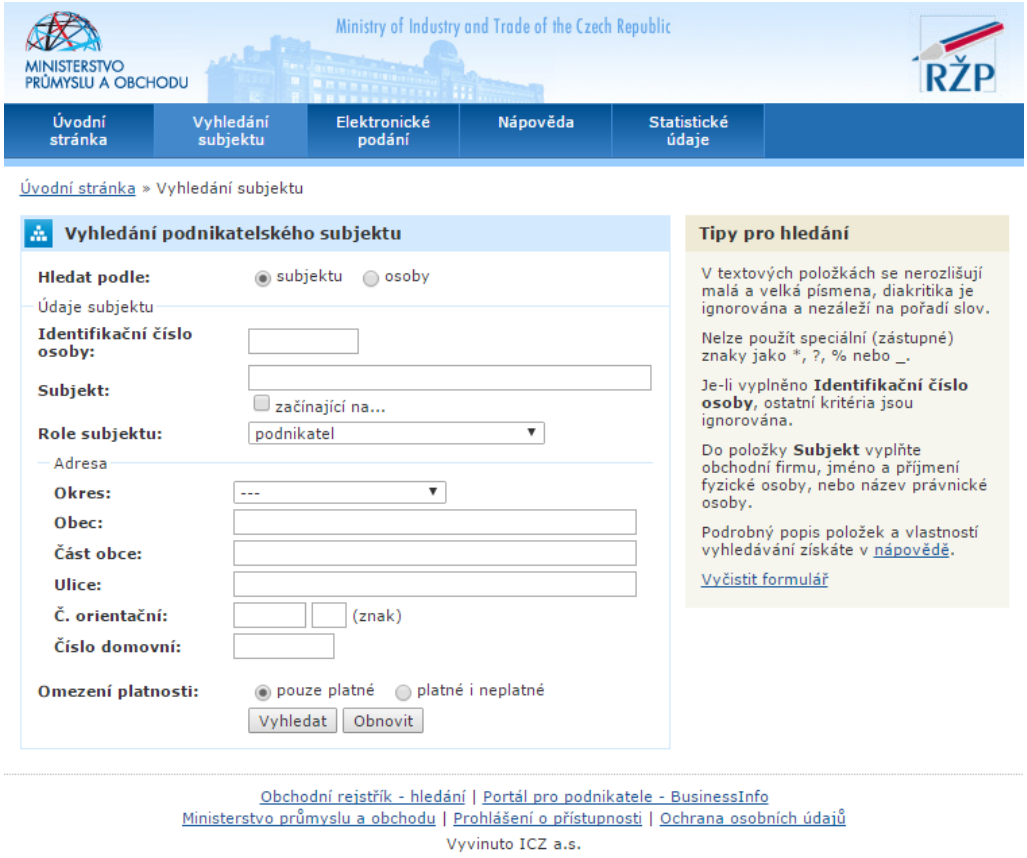
Pro zvýšení bezpečnosti používání platebních karet slouží Fraud monitoring. Proces spočívá v ověřování nezvyklých transakcí zaznamenaných systémem FDS. V případě neobvyklého chování klienta se pracovník banky pokusí telefonicky spojit držitele karty k ověření neobvyklých transakcí. Pokud se nepodaří s klientem spojit, má banka právo kartu zablokovat, a to i bez jeho vědomí. Zamezí se tím dalšímu možnému zneužití. V případě zjištění podvodných transakcí je klient zařazen na černou listinu, tedy black list. Tento systém je velmi podstatný, protože každým rokem dochází ke zvyšování karetních podvodů a tedy i ztrát pro bankovní instituce.

5.8.7 Early Fraud Detection

Early Fraud Detection je nástroj, který má za úkol odhalit podvod co nejdříve poté, co nastal, včasným odhalením pak snižujeme případnou ztrátu a předcházíme jeho opakování. Tento prostředek se využívá především u interních a organizovaných podvodů, naopak příliš nefunguje u jednorázových neorganizovaných podvodů. Princip spočívá

v analýze všech interních a externích zdrojů. Interní informace jsou zejména klientské údaje, aplikační žádosti, transakční historie a databáze podvodů, jejíž pomocí nacházíme vhodná schémata podvodu. „Externími zdroji jsou pak například informace z CCB (úvěrový registr), informace třetích stran (např. policie), veřejné seznamy a rejstříky (zejména Obchodní rejstřík, Živnostenský rejstřík, portál Plátci DPH, atd.).“[16] Základní princip je výběr klientů z databáze podvodů a dodání všech dat ohledně podvodu. Ve výběru dat pak vyhledáváme shodné matice chování klientů, pomocí nich pak vytváříme tzv. scénáře pro zjednodušení budoucí detekce.

Obrázek 14 Živnostenský rejstřík



Zdroj: http://www.rzp.cz/cgi-bin/aps_cacheWEB.sh?VSS_SERV=ZVWSBJFND

[16] Čírtková, Ludmila. Podvody, zpronevěry, machinace. 2005. str. 54

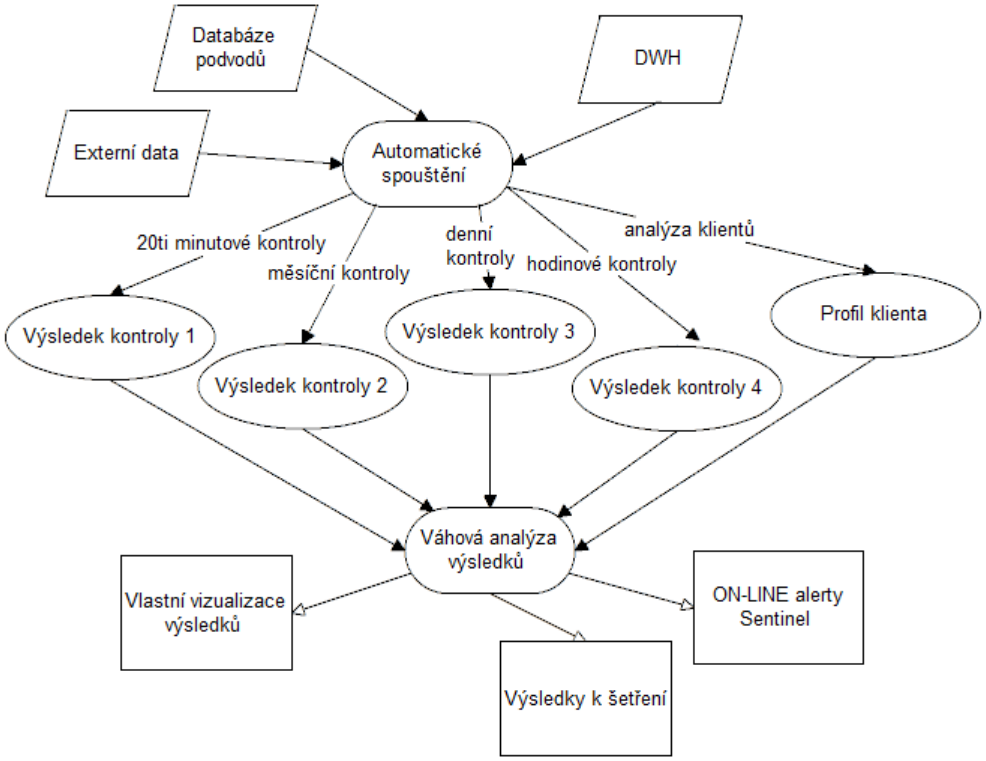
5.8.7.1 Scénáře podvodů

Scénářů existuje celá řada a stále nové vznikají. Prověřují se například zaměstnanci s rizikovým profilem, tzn. s vysokým počtem úvěrů, zaměstnanci v exekučním řízení, zvýšený počet nedoručených výpisů nebo ztracené dokumentace k produktům poskytnutým jedním zaměstnancem. Je třeba sledovat i transakční chování, je třeba mít přehled nad klienty s vyšším počtem transakcí, vkladů nebo výběrů hotovosti. Pozorujeme tak rizikové chování, jako je gambling, hraní hazardních her, atd. Také sledujeme pohyb nežádoucích osob, jako osoby na black listech, podezřelý je jejich vstup do firmy krátce před nebo po čerpání úvěru. V neposlední řadě kontrolujeme platby na účty Ministerstva financí, zda klient řádně platí daně.

5.8.8 Expertní scénáře

Expertní scénáře jsou tvořeny na základě určitých souvislostí, nelze je tvořit nezávisle na jiných scénářích. Dnes již není tolik nutné tvořit nové scénáře, existuje jich velké množství, více se využívá kombinace několika scénářů najednou, lépe řečeno jejich výsledků. Spojením scénářů můžeme odhalit náznaky podvodů, kterých bychom si nevšimli v případě, že bychom s nimi pracovali zvlášť. Rizikovost klienta vyhodnocuje mechanismus, které můžou vypadat například takto:

Obrázek 15 Expertní scénář



Zdroj: http://www.business-continuity.cz/cc-21-6-ucinnych-nastroju-prevence-a-detekce-podvodu---zkusenosti-z-praxe.php

5.8.9 Prověření podezřelých osob a společností

Výstupy z jednotlivých postupů detekce srovnáváme pomocí interní aplikace banky. Osobní údaje klienta z vyplněné žádosti porovnáváme s informacemi v databázích, ať už v naší interní databázi nebo v jiných nám přístupných externích zdrojích. Tím může být například Registr ekonomických subjektů, webové portály Ares nebo Justice, ŽR nebo OR, Česká advokátní komora nebo Centrální registr dlužníků. Poté vyhodnotíme, zda údaje souhlasí či nikoli. Pokud odhalíme podvodné jednání, osoba či společnosti je vložena na black list.

Obrázek 16 Internetový portál justice.cz

Zdroj: https://or.justice.cz/ias/ui/rejstrik-$firma

5.8.10 SWOT Analýza

„Tato analytická technika vyhodnocuje bankovní instituci z hlediska fungování v procesu detekce a prevence podvodů. Cílem je srovnání silných a slabých stránek, příležitostí a hrozeb banky a výsledné vyhodnocení.“[17]

Silné stránky zahrnují využití dostupných metod pro detekci a prevenci. Čím více metod banka používá, tím lépe. Kromě zmíněných metod sem lze zahrnout například školení zaměstnanců v oblasti detekce a prevence podvodů, zapojení specialistů nebo využití scanu dokladů.

Slabými stránkami pro boj s bankovními podvody jsou převážně chyby zaměstnanců, ať už nedbalý přístup při sepisování žádostí nebo přehlédnutí podezřelých informací v žádostech. Problém nastává u mobilních telefonních čísel, které nelze prověřit

[17] Smejka, V. Řízení rizik ve firmách a jiných organizacích. 2013. s. 64

v telefonním seznamu. Dalšími problémy může být výpadek sítě nebo nekvalitní využití nástrojů detekce.

Příležitosti banky spočívají ve využívání a vylepšování prostředků prevence a detekce podvodů, například vylepšování systémů FDS nebo zdokonalování systémů selektů (neboli dotazů SQL). Příležitostí je pro nás i spolupráce s ostatními finančními institucemi a vzájemné sdílení údajů o podvodech

Hrozbami jsou pro banku podvody samotné, tedy jejich činitelé. Využitím black listů a jiných nástrojů zabráníme hrozbě poskytnutí úvěru problémovým klientům, avšak hrozba zde číhá v podobě nových druhů podvodů, které jsme prozatím našimi prostředky neodhalili.

Obrázek 17 SWAT analýza

	Pomocné pro dosažení cíle	**Škodlivé** pro dosazení cíle
Vnitřní prostředí	**SILNÉ STRÁNKY** (S - strenghts)	**SLABÉ STRÁNKY** (W - weaknesses)
Vnější prostředí	**PŘÍLEŽITOSTI** (O - opportunities)	**HROZBY** (T - threats)

Zdroj: http://en.wikipedia.org/wiki/Bank_fraud

5.9 Prověřování podezřelých žádostí

Žádosti se prověřují porovnáním údajů z žádosti, popřípadě smlouvy, v interní aplikaci s údaji v externích databázích. Zjištěné nesrovnalosti se dále ověřují a výsledně vyhodnotí. Příkladem podezřelých informací je například odlišné zadání zaměstnavatele, telefonního čísla nebo příjmu. Smlouvy se vyhodnocují jako podvodné, pokud klient nesplácí úvěr, na kontaktním telefonním čísle klienta nelze zastihnout nebo číslo vůbec neexistuje. Zejména pak prověřujeme pracovní poměr uvedený v žádosti, zda klient na uvedeném působišti pracoval nebo pracuje, zejména v době uzavírání smlouvy. V případě

padělání dokladů odhalíme v procesu prověřování žádostí, že některé údaje v smlouvě nesouhlasí. Vyžitím externích systémů detekujeme klienty ve výkonu trestu, klienty pobývající dlouhodobě v cizině nebo klienty zadlužené u jiných finančních institucí.

Při odhalení podvodného jednání vkládáme osob či organizaci na black list. Případ se předá trestnímu oddělení, které podává trestní oznámení na danou osobu či subjekt.

5.10 Živnosti a společnosti

Podezřelé živnosti se vyznačují například přerušením živnosti a následné hromadění žádostí o úvěr na IČ zrušené živnosti. Podezřelé je zejména zvýšený počet žádostí spadající pod jednu živnost nebo podobně vyplněné žádosti (např. uvedená výše příjmu).

U společností se zaměřujeme na časté změny majitele společnosti nebo statutárního orgánu. Společnosti mohou využívat tzv. bílé koně, kdy je společnost převedena na nového majitele, většinou donucením nebo za úplatu, který kryje skutečného pachatele podvodu. Mezi podezřelé řadíme i společnosti s nulovými finančními prostředky, které fyzicky nepodnikají.

„Ověřování probíhá vyhledáním společnosti v obchodním rejstříku a porovnáním nalezených údajů s údaji uvedenými v žádosti, zejména název a adresa společnosti. V rejstříku si také ověříme odkdy je společnosti aktivní a zda-li není v konkursu či likvidaci, sledujeme aktuální změny ve statutárním orgánu subjektu.“[18]

Živnosti prověřujeme velmi obdobně, ale s využitím Živnostenského rejstříku. Zaměřujeme se na místo, obor a předmět podnikání, zahájení provozování, popř. přerušeni.

5.11 Analýza

Analýza využívá poznatky ze systémů FDS, které využívá k rozboru profilu podvodníků. Napomáhá v detekci podvodných žádostí, v podstatě znemožní podezřelým žádostem, aby prošly schvalovacím řízením. Cílem je odhalit podvodné jednání co nejdříve po poskytnutí, ideálně ještě dříve. Analytická práce je zde založena na vytváření tzv.

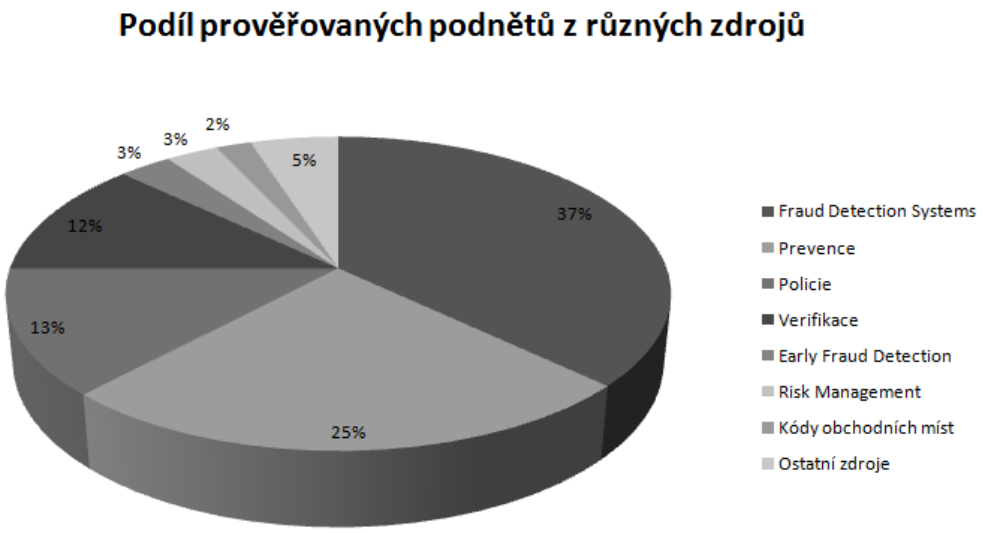
[18] Čírtková, Ludmila. Podvody, zpronevěry, machinace. 2005. str. 57

selectů pomocí příkazů SQL. Z poznatků předešlých podvodů definujeme jejich charakteristické znaky, z těch jsou tvořeny selecty pro výběr klientů ze seznamu žadatelů. Získaná data použije oddělení prevence k ověření podezřelých osob.

5.12 Využití nástrojů detekce

V následném grafu je vyjádřeno využívání jednotlivých nástrojů detekce. Je patrné, že se nejvíce využívá systému na odhalování podvodů, neboli FDS, a významným prvkem je i proces prevence.

Graf 4 Zdroje prověřovaných podnětů



Zdroj: http://www.aec.cz/index.php?id=585,1050,0,0,1,0

6 Návrh a využití scénáře podvodů

Aplikací nástroje EFD (Early Fraud Detection) vytváříme určité schéma podvodu, které pak využijeme k posouzení věrohodnosti nových žádostí klientů. Takovýchto schémat existuje celá řada, liší se zaměřením na určitý druh podvodu. Zaměříme se na případ, kdy dochází k nárůstu počtu žádostí spadající pod určitého zaměstnavatele, tedy společnost, jejíž zaměstnanci v poslední době žádají o úvěr ve velkém měřítku. Podezřelé jsou zejména ty, u kterých se dříve žádosti téměř nevyskytovaly, tedy na vysoký podíl celkových a nových žádostí. V tomto případě se může jednat o podvodnou společnost, která vznikla za účelem krytí podvodné činnosti.

Máme tedy databázi klientů, kde uchováváme informace uvedené v jejich žádostech. Pro přiblížení zde máme zjednodušenou tabulku zaměstnavatelů. Tedy pokud klient uvede potřebné informace o svém zaměstnavateli, jeho údaje se uloží do zvláštní tabulky.

Tabulka 4 Zaměstnavatelé

ico_zam	nazev_zam	ulice_zam	telefon_zam	c_uctu_zam	zadosti_celkem	nove_zadosti
00514578	Barvy, s.r.o.	Radlická 153/7	281975447	5748980123/0303	5	1
01575015	Auta, a.s.	Korunní 17	736858411	2599014855/0200	2	NULL
20575807	Product, s.r.o.	Levá 250/13	281945588	5952001454/0300	12	NULL
15897001	V.I.P., s.r.o.	Slezská 135/2	281926558	2592201456/0300	3	1
02489845	PoP, a.s.	Korunní 17	281925700	2114969011/0200	1	8

V tabulce je uveden počet žádostí, u kterých je daný zaměstnavatel uveden ve spojitosti s žadatelem o úvěr. Žádosti jsou rozděleny z časového hlediska na žádosti celkové a nové, přičemž jako nové považujeme ty, které nejsou starší než dva měsíce.

Samotné žádosti jsou ukládány do tabulky „Žádosti“, kde je kromě data uzavření a čísla žádosti uveden klíč k tabulce klientů a zaměstnavatelů. Z této tabulky jsou tedy sčítány žádosti spadající pod určité zaměstnavatele.

Tabulka 5 Žádosti

id_zadosti	rodne_cislo_kl	ico_zam	datum
0158714	900418/1589	00514578	16-03-01
0158715	815706/4684	01575015	16-03-01
0158716	715914/8459	20575807	16-03-02
0158717	840827/4875	15897001	16-03-03
0158718	740201/6985	02489845	16-03-03

Je třeba si předem stanovit poměr nových žádostí za určité období oproti všem žádostem na daného zaměstnavatele. Řekněme tedy, že považujeme za dostatečně reprezentující 20% nárůst nových žádostí oproti celkovému počtu žádostí na jednoho zaměstnavatele. Vybíráme tedy z tabulky ty zaměstnavatele, u kterých je poměr větší než 80%. Pro přesnější výsledek je pak vhodné stanovit délku období, za které se budou žádosti sčítat. V praxi se nejčastěji pracuje s rozmezím dvou měsíců. Aby byl výběr co nejvíce funkční, je třeba zadávat časové údaje, tady datum, vždy ve stejném formátu.

Příkaz takového výběru může vypadat například takto:

```
SELECT nove_zadosti, zadosti_celkem
FROM (SELECT COUNT id_zadosti as nove_zadosti
        FROM zadosti
        WHERE datum_zadosti > (16-03-01)
        GROUP BY zadosti.ico)
nove_zadosti INNER JOIN
        (SELECT COUNT id_zadosti
        AS zadosti_celkem
        FROM zadosti
        WHERE datum_zadosti > (15-03-01)
        GROUP BY zadosti.ico)
        historicke_zadosti
ON nove_zadosti.id_zadosti=zadosti_celkem.id_zadosti
WHERE nove_zadosti/zadosti_celkem > 0.8;
```

Pokud tento select aplikujeme na vzorovou tabulku zaměstnavatelů, výsledný výběr nám vyhodnotí zaměstnavatele „PoP, a.s.“ jako rizikového.

Výsledek ještě porovnáme s tabulkou Blacklist, ve které shromažďujeme údaje o společnostech, které se již v minulosti účastnily nějakého podvodu. Obsahuje atribut IČO, dle kterého firmu vyhledáváme, dále například název společnosti, datum zařazení na blacklist a nějaký kód spáchaného podvodu, dle kterého si pak vyhledáme o jakou trestnou činnost šlo.

Tabulka 6 Blacklist

ico	nazev	datum_zarazeni	kod_podvod
01568452	Wind, a.s.	15-09-21	503
25219968	Reality, s.r.o.	13-04-11	404
25482247	SmartTV, s.r.o.	15-01-30	502
10588513	Matrace, s.r.o.	14-12-01	502
02489845	PoP, a.s.	14-04-17	404

Firmu, kterou jsme vyhodnotili jako rizikovou, zkusíme vyhledat pomocí příkazu:

SELECT nazev FROM blacklist WHERE ico=02489845;

Pokud firmu nalezneme v blacklistu, můžeme si být zas o něco víc jistí, že jde o podvodnou společnost a případ předáváme týmu Investigace k prověření.

7 Závěr

Z důvodu dostupnějších podmínek pro získání úvěru, s nástupem elektronického bankovnictví a celkově s vývojem technologií se objevuje stále více příležitostí k páchání podvodů v bankovním sektoru. Pachatelé se snaží využít slabé stránky banky a tím získat finanční prostředky. Banky využívají všemožné prostředky k odhalování této činnosti. Kvalitní detekční systém může být pro banku přínosný z hlediska ochrany svého majetku, ale také jako konkurenční výhoda, neboť klient raději zvolí banku, která má dostatečně nastavená opatření proti neoprávněným transakcím případnému zneužití platební karty.

Cílem této bakalářské práce bylo vytvořit scénář podvodu, jehož pomocí můžeme detekovat podvodnou činnost v prostředí banky. Pro tento účel jsem vytvořila fiktivní databázi s informacemi o klientech banky a pomocí návrhu výběru určitých dat demonstruji průběh ověřování klienta.

Tato činnost je v praxi velmi různorodá, záleží na nashromažďovaných datech instituce, rozsahu detekčních prvků a na vlastních návrzích specialistů. Proto je velmi důležité sdílení informací mezi bankami, aby měli co nejvíce informací o kriminální činnosti v tomto odvětví. Také proto, že pachatelé zkoušejí operovat ve více institucích najednou.

Vhodným řešením by mohla být databáze podvodů, na kterou by měly banky napojené systémy, kde by sdílely informace o uskutečněných podvodech. Překážkou je však stále znění zákona č. 101/2000 Sb., o ochraně osobních údajů a bankovní tajemství. Banky tedy musejí zachovávat mlčenlivost ohledně klientských údajů, pokud klient nedá souhlas k jejich sdílení. Banky tedy mohou informace poskytovat pouze státnímu zastupitelství či soudu.

8 Citovaná literatura

8.1 Bibliografie

1. Kroenke, David a Auer, David. ***Databáze***. místo neznámé : Computer Press, 2015. ISBN 9788025143520.
2. Lacko, Ľ. ***SQL: hotová řešení pro SQL Server, Oracle a MySQL***. Brno : Computer Press, 2003. 80-7226-975-5.
3. Veselá, Judita. ***Relační databáze jako nástroj pro analýzu a prezentaci dat.*** 2014. 978-80-86847-73-3.
4. T., Conolly. ***Mistrovství - Databáze: Profesionální průvodce tvorbou efektivních databází.*** 2009. 978-80-251-2328-7.
5. Lacko, L. ***Business Inteligence v SQL Serveru 2008***. 2009. 978-80-251-288-9.
6. Molinaro, A. ***SQL: Kuchařka programátora.*** 2009. 978-80-251-2617-2.
7. Oppel, A. ***Databáze bez předchozích znalostí***. 2006. 978-80-251-1199-7.
8. Smejka, V. ***Řízení rizik ve firmách a jiných organizacích***. 2013. 978-80-247-4
9. Čírtková, Ludmila. ***Podvody, zpronevěry, machinace***. 2005. 80-86795-12-8.
10. Polouček, S. ***Bankovnictví.*** 2006. 80-7179-462-7.
11. James, L. ***Phishing bez záhad***. Praha : Grada Publishing, 2007. 978-80-247-1766-1

8.2 Webové stránky

1. http://www.databaze.chytrak.cz/modely.htm
2. http://www.dotnetportal.cz/clanek/60/Lehky-uvod-teorie-databazi
3. http://gml.vse.cz/data/oppa-webdesign/zaklady-db.html
4. http://www.itnetwork.cz/ms-sql
5. http://business.center.cz/business/pravo/zakony/trestni_zakon/cast2h9.aspx
6. http://en.wikipedia.org/wiki/Bank_fraud
7. http://www.aec.cz/index.php?id=585,1050,0,0,1,0
8. http://www.gfo.cz/page.php?show=vzdelani&id=5&PHPSESSID=964332471e26553e61e097e1a11017dd
9. https://www.fiserv.com/customer-channel-management/online-banking/fraud-detection-system.aspx

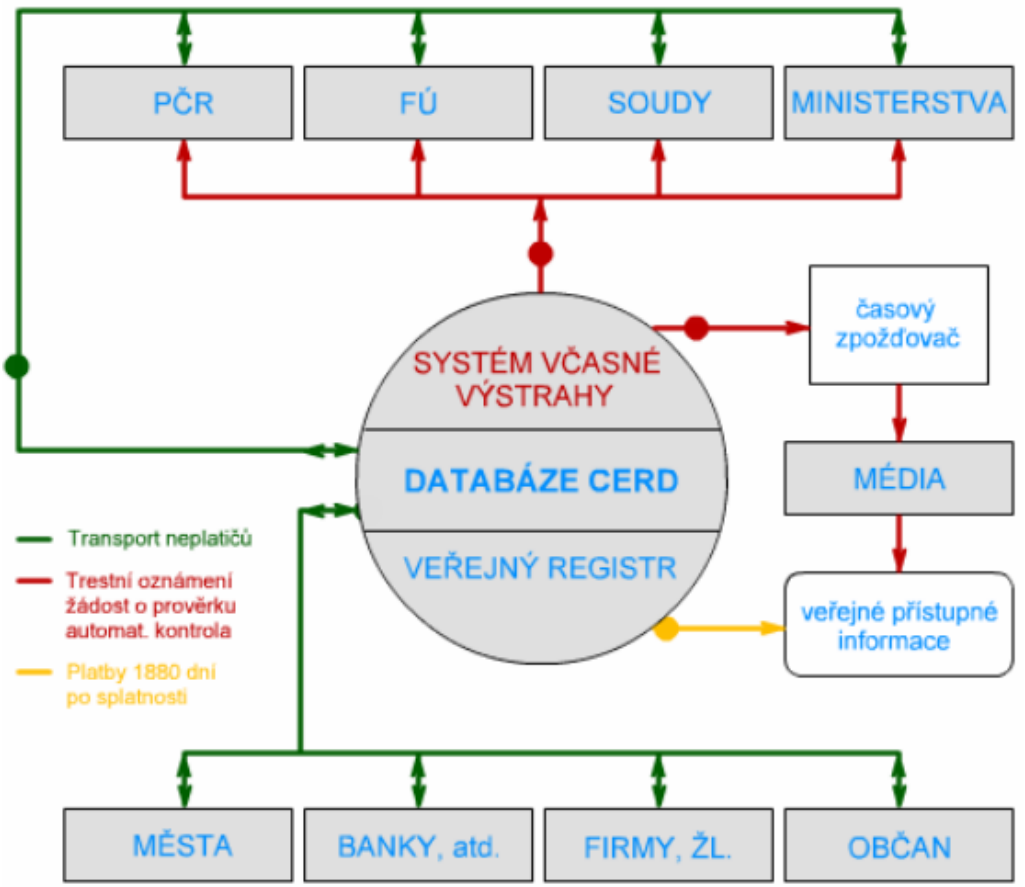
9 Seznam obrázků

10 Seznam Tabulek

11 Seznam Grafů

12 Seznam příloh

Fungování systému CERD



Vzor žádosti o poskytnutí úvěru

Žádost o poskytnutí kontokorentního úvěru

Fio banka, a.s.
IČ 61858374, Praha 1, V Celnici 1028/10, PSČ 117 21.
Zapsaná v obchodním rejstříku vedeném rejstříkovým soudem v Praze, spis. zn. B, vložka 2704.

Číslo žádosti: ☐☐☐☐☐☐☐ (vyplní banka)

žadatel – majitel účtu

Jméno a příjmení:[7]		**Pohlaví:** **Stát. přísl.:**[1]	**Místo narození:**	**R. č.**[2]**/IČ:**[8]
Trvalý pobyt: Ulice + č.p.		**Město, obec:**	**PSČ:**	**Stát:**
Politicky exponovaná dle zákona 253/2008 sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti:				
Korespondenční adresa:[3] Ulice + č.p.		Město, obec:	PSČ:	Stát:
Telefon:	Mobilní telefon:	Fax:	E-mail:	
Druh průkazu totožnosti:[4]	Číslo:	Země vydání:[1]	Platný do:	Vydal:
Druh průkazu totožnosti:[9]	Číslo:	Země vydání:[1]	Platný do:	Vydal:

Přidělené číslo klienta:

Zastoupen:[5] Jméno a příjmení/Obchodní firma/Název:		Pohlaví:[6]	Místo narození:[6]	R. č.[2]/IČ:	Druh oprávnění:
Trvalý pobyt/Sídlo: Ulice + č.p.		Město, obec:	PSČ:	Stát:	Stát. přísl.:[1,6]
Údaje o průkazu totožnosti:[6]					
Druh průkazu totožnosti:[4]	Číslo:	Země vydání:[1]	Platný do:	Vydal:	
Druh průkazu totožnosti:[7]	Číslo:	Země vydání:[1]	Platný do:	Vydal:	

Číslo účtu, k němuž je poskytnutí kontokorentního úvěru požadováno: _____ / 2010

Úvěrový rámec:

požadovaná výše: _____

minimální výše: _____

Sazba poplatků za kontokorentní úvěr:

☐ **Roční – sazba 1 (Tarif „Roční 1")**
☐ **Roční – sazba 2 (Tarif „Roční 2")**
☐ **Roční – sazba 3 (Tarif „Roční 3")**

☐ **Nový úvěr** ☐ **Navýšení stávajícího úvěru** ☐ **Změna tarifu stávajícího úvěru**

Na účet, ke kterému žádám o poskytnutí kontokorentního úvěru, jsou posílány tyto pravidelné platby - příjmy majitele účtu:

Příjem	Průměrná měsíční výše	Odesílatel
Čistá mzda		
Důchod nebo renta		
Sociální dávky		
Jiné (uveďte jaké)		
Jiné (uveďte jaké)		

1) zkratka státu dle Seznamu, 2) není-li, datum narození, 3) není třeba vyplňovat, je-li shodná s adresou trvalého pobytu, 4) občané zemí EU občanský průkaz nebo pas, ostatní cestovní pas, 5) vždy osobně přítomný zástupce klienta (právnická osoba je osobně přítomna, jedná-li za ni osobně přítomný statutární orgán); další údaje o zástupci uveďte v příloze, 6) pouze fyzická osoba 7) druhý průkaz totožnosti je-li vyžadován

1/2

☐ Prohlašuji, že nejsem držitelem platného oprávnění podnikat

☐ Prohlašuji, že jsem držitelem platného oprávnění podnikat podle

- ☐ živnostenského zákona,
- ☐ zákona o zemědělství,
- ☐ dle jiných zákonů než živnostenského a zákona o zemědělství

a v současné době

- ☐ vykonávám podnikatelskou činnost v oboru:
- ☐ webové stránky mé k podnikatelské činnosti:
- ☐ mám přerušeno podnikání,
- ☐ tuto podnikatelskou činnost nevykonávám, ale nemám přerušeno podnikání

Přehled stávajících úvěrů a jiných závazků:

Typ úvěru / závazku	Věřitel	Celková výše	Aktuální zůstatek	Měsíční splátka	Splatnost

Prohlášení majitele účtu:

Žádám o poskytnutí výše specifikovaného typu kontokorentního úvěru s požadovaným úvěrovým rámcem. Nebude-li možno vyhovět mé žádosti o poskytnutí kontokorentního úvěru s požadovaným úvěrovým rámcem, žádám o poskytnutí kontokorentního úvěru s co možná nejvyšším úvěrovým rámcem, nejméně však ve výši uvedeného minimálního úvěrového rámce.

Čestně prohlašuji, že (prosím zaškrtnout)

☐ nemám nesplacené závazky vůči jakémukoliv finančnímu úřadu, vůči české správě sociálního zabezpečení, ani vůči své zdravotní pojišťovně,

☐ nemám žádné závazky po splatnosti vůči bankám či jiným věřitelům mimo závazků po splatnosti uvedených v této žádosti,

☐ nemám závazky s hrozící žalobou či hrozícím vymáháním, a nejsou mi známy žádné okolnosti, které by mohly některou z výše uvedených situací způsobit,

☐ na moji osobu nebo majetek k dnešnímu dni nebyl podán návrh na zahájení insolvenčního řízení, návrh na výkon soudního nebo jiného rozhodnutí nebo exekuci, a nejsou mi známy žádné okolnosti, které by mohly některou z výše uvedených situací způsobit,

☐ nejsem účastníkem žádného soudního sporu, rozhodčího nebo správního řízení, které by mohlo negativně ovlivnit nebo ohrozit platnost nebo vymahatelnost budoucích závazků,

☐ jsem nebyl pravomocně odsouzen za jakýkoli trestný čin, a že proti mé osobě není v současné době vedeno trestní stíhání,

☐ nebyla omezena má způsobilost k právním úkonům,

☐ mé příjmy neplynou z jakýchkoliv nelegálních nebo nezákonných aktivit a ani se žádných nelegálních nebo nezákonných aktivit nedopouštím,

☐ že jsem schopen úvěr, o který žádám, řádně splácet.

Komentář k nezaškrtnutým výše uvedeným prohlášením:

Dále prohlašuji, že jsem se seznámil s aktuálním zněním Předsmluvních informací o spotřebitelském úvěru.

Prohlašuji, že všechny údaje uvedené na žádosti jsou úplné a pravdivé, a zároveň se zavazuji neprodleně hlásit veškeré jejich změny.

_____, dne _____

....

za banku klient

Příloha 3

Registr plátců DPH

Údaje o registrovaném subjektu

DIČ:	**CZ24307416 Právnická osoba**
Obchodní firma / název:	**COMPWARE s.r.o.**
Sídlo:	**Pobřežní 249/46** **PRAHA 8 - KARLÍN** **186 00 PRAHA 86**

Finanční úřad pro hlavní město Prahu
Územní pracoviště pro Prahu 8, Trojská 13a, PRAHA 8, tel.: 266 013 111
Údaje zobrazeny dne 13.03.2016

Údaje o nespolehlivém plátci DPH

Nespolehlivý plátce:	**NE**

Bankovní účty určené ke zveřejnění

	Datum zveřejnění
2100264950/2010	**01.04.2013**

Údaje o registraci k DPH

Typ registrace	Registrace platná od:	Registrace platná do:
Plátce	**04.06.2012**	