ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Bakalářská práce

Analýza metod a nástrojů fraud managementu ve vybraném podniku

Analysis of methods and tools of fraud management in a selected company

Jan Čihák

Plzeň 2014

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta ekonomická
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan ČIHÁK**
Osobní číslo:	**K11B0134K**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika a management**
Název tématu:	**Analýza metod a nástrojů Fraud Managementu ve vybraném podniku.**
Zadávající katedra:	**Katedra financí a účetnictví**

Zásady pro vypracování:

1. Proveďte analýzu metod a nástrojů řízení rizik podvodů (Fraud Managementu) a komparaci jejich předností a omezení.
2. Definujte rizika, se kterými se v oblasti Fraud Managementu potýká bankovní sektor a zhodnoťte možnosti minimalizace finanční kriminality v této oblasti.
3. Ve stručnosti představte podnik a jeho core aktivity, činnosti a procesy.
4. Zhodnoťte metody a nástroje Fraud Managementu využívané ve společnosti UniCredit, případně navrhněte možná zlepšení.

Rozsah grafických prací: **neuveden**

Rozsah pracovní zprávy: **40 - 60 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

- **ČÍRTKOVÁ, Ludmila. a kol.** *Podvody, zpronevěry, machinace (možnosti prevence, odhalování a ochrany před podvodným jednáním).* **Praha: Armex Publishing, 2005. ISBN 80-86795-12-8**
- **NIGRINI, Mark.** *Forensic analytics. Methods and Techniques for Forensic Accounting Investigations.* **Wiley Corporate F&A, 2011. ISBN 978-0-470-89046-2**
- **SILVERSTONE, Howard; SHEETZ, Michael.** *Forensic Accounting and Fraud Investigation for Non-Experts. 2nd ed.* **WILEY, 2007. ISBN 0-471-78487-7**

Vedoucí bakalářské práce: **Ing. Veronika Burešová**
Katedra financí a účetnictví

Datum zadání bakalářské práce: **1. června 2013**

Termín odevzdání bakalářské práce: **6. prosince 2013**

Doc. Dr. Ing. Miroslav Plevný
děkan

L.S.

Prof. Ing. Lilia Dvořáková, CSc.
vedoucí katedry

V Plzni dne 1. června 2013

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma

„Analýza metod a nástrojů fraud managementu ve vybraném podniku“

vypracoval samostatně pod odborným dohledem vedoucí bakalářské práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni, dne 22. dubna 2014 ……

podpis autora

Obsah

Úvod

Cílem mé bakalářské práce bude klasifikace metod a nástrojů fraud managementu, kterými se bankovní dům brání podvodům a machinacím finančního charakteru. Vzhledem k velkému rozsahu tématu je práce zaměřena především na oblast praní špinavých peněz a financování terorismu a dále na popis postupů a možností prevence v oblasti platebních karet.

Fraud management jako takový obsahuje nepřeberné množství technik, metod a nástrojů k prevenci a odhalování pokusů o finanční výhodu některých jedinců či celých organizovaných skupin. Banka jako taková je neustále, každodenně, vystavována těmto pokusům a to jak zvenčí, tak zevnitř. Navíc je v tomto boji zapojeno množství moderní techniky, která může skýtat nejednu bezpečnostní mezeru. Firemní procesy a metody tak musí být neustále aktualizovány a vylepšovány o nové poznatky. Je to nikdy nekončící boj proti mnoha nepřátelům, které se díky rozvoji fraud managementu snaží bankovní domy zastavit nebo alespoň minimalizovat.

Práce má za úkol definovat a analyzovat tyto metody a nástroje a nastínit jejich jednotlivá úskalí a etapy. Zaměřena je především na nejnovější typy metod prevence, obrany, detekování, vyhodnocení a řešení finančních podvodů kolem platebních karet, elektronických platebních příkazů a oblasti praní špinavých peněz a financování terorismu. Všechny tyto postupy jsou velmi aktuální a řadí se ke klíčovým prioritám při definování řízení fraud managementu banky.

Vybranou společností k vypracování praktické části je banka UniCredit Bank Czech Republic and Slovakia, a.s. (dále jen UniCredit), kde jsem od roku 2007 zaměstnán a zde jsem i zjišťoval zavedení a používání metod a nástrojů řízení rizik a prevence podvodů.

Hlavním důvodem proč jsem si toto téma vybral, je tak má praxe ve finančním oboru, potažmo zpracování elektronických plateb. Momentálně pracuji na oddělení zahraničního platebního styku. V předchozím zaměstnání jsem se věnoval problematice elektronického bankovnictví. Obě moje poslední zaměstnání tak úzce působí s uvedenou tématikou a já mohu využít svoje zkušenosti z tohoto působení.

K vypracování jsem využil domácí i zahraniční odbornou literaturu, zdroje z internetu, prezentace a konzultace s odborníky v naší společnosti.

1 Co je podvod

Podvod je činnost, která se odehrává v sociálním prostředí a má vážné následky pro ekonomiku, podniky a jednotlivce. Jedná se o jeden z druhů trestných činů patřící do kategorie majetkové kriminality. Finanční podvod můžeme pak definovat jako útok proti společnosti či jednotlivci, jehož výsledkem je finanční ztráta. Americká Asociace certifikovaných vyšetřovatelů podvodů (ACFE) dále definuje pracovní podvody jako: "využití zaměstnání pro osobní obohacení prostřednictvím záměrného zneužití nebo nesprávného použití prostředků zaměstnávající organizace nebo aktiva." Moderní definice podvodu je odvozena především z trestního zákoníku, ale mnoho starých prvků stále přetrvává. Původ slova fraud můžeme také hledat v latinském *fraus,* což v překladu znamená darebáctví, poškození nebo právě podvod. [5]

Právní definici podvodu najdeme v zákoně č. 40/2009 Sb., trestního zákoníku, který vstoupil v platnost 1. ledna 2010. Ten uvádí v §209 podvod jako trestný čin, jehož se dopustí ten, 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. Za takové jednání hrozí trestem až na dva roky nepodmíněně a zákazem činnost, propadnutím věci nebo jiné majetkové hodnoty. Zároveň je však trestná i pouhá příprava podvodu. (Zákon č. 40/2009 Sb. Trestní zákon)

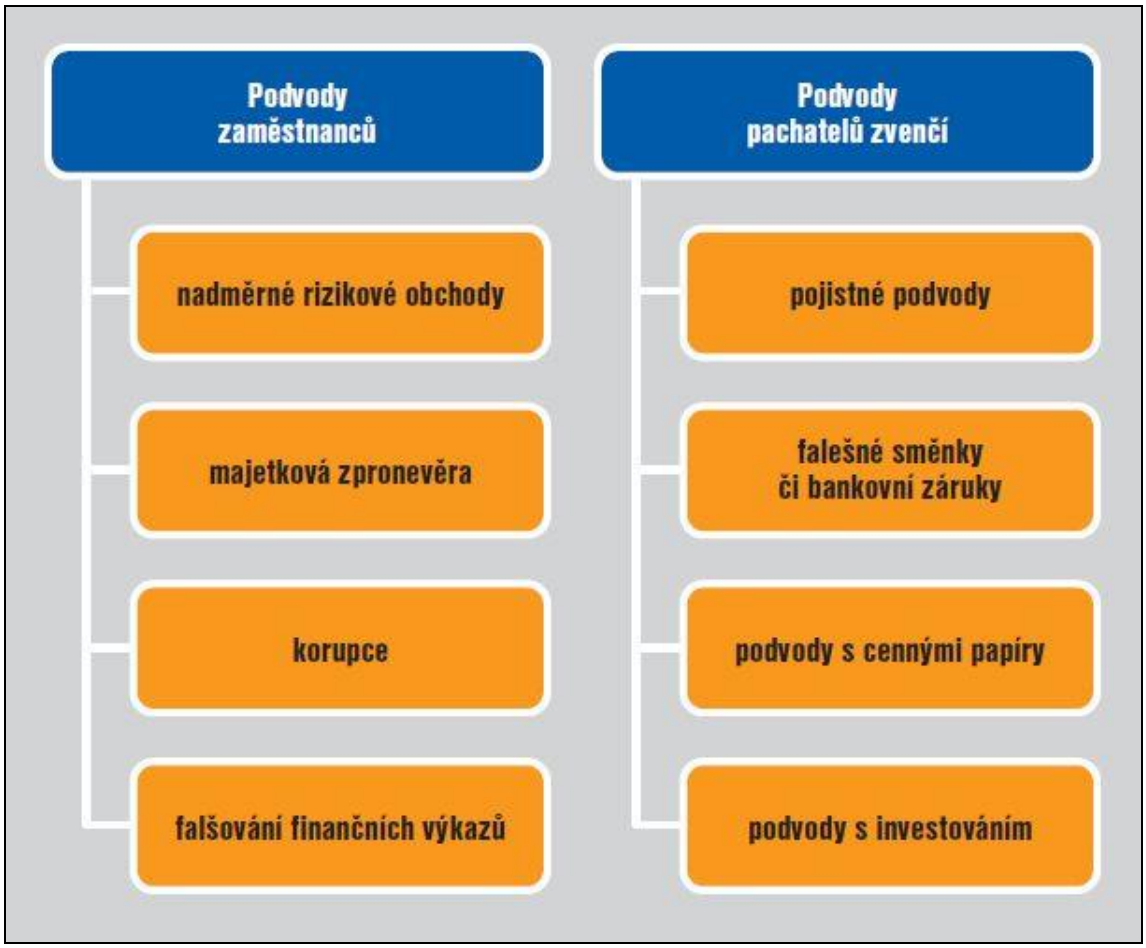
Podvody však nemusejí mít jen formu přímého zneužití peněz nebo majetku. Je třeba si dávat pozor i na ostatní formy podvodného jednání, které jsou v praxi posuzovány jako trestný čin. Jde kupříkladu o případy, kdy zaměstnanec využije ke škodě zaměstnavatele jeho prostředky a způsobí mu tak újmu na majetku přesahující 5.000 Kč. Může to být využití telefonních linek, přístupu na internet, nebo televizního vysílání, kdy dotyčný předstírá, že jedná v zájmu zaměstnavatele. [1]

1.1 Typy podvodů

Finanční podvody lze rozdělit do dvou skupin podle hlediska, kdo je pachatelem: podvody zaměstnanců a podvody spáchané pachateli zvenčí.

Samostatně stojí počítačové podvody, praní špinavých peněz, financování terorismu, krádeže identity a různá další podvodná jednání. Detailní rozdělení můžeme vidět na obrázku číslo 1.

Obr. č. 1: Typy podvodů



zdroj: [6]

1.2 Podvody zaměstnanců

Ze své podstaty jsou velmi nebezpečné z důvodu detailní znalosti prostředí uvnitř instituce. Zaměstnanec má tak více informací a možností, než pachatel zvenčí. Dle zastávané pozice je tedy pachatel schopen napáchat rozsáhlé škody a navíc má mnohdy i možnost po sobě zahladit stopy a důkazy. Z tohoto hlediska je nejdůležitější prevence. Tam kde nemůže

zaměstnanec jednat sám nebo bez kontroly, tam je pro něj větší problém způsobit vědomě finanční podvod. Bohužel se však i rozmáhají podvodná jednání přímo od pracovníků, kteří bezpečnostní standardy nastavují a řídí. V tom případě musí vždy fungovat jak automatické detekce, tak následné kontroly, například v podobě finančního auditu. Podvody zaměstnanců jsou čím dál více sofistikované a úkolem fraud managementu je především identifikace příležitostí, tedy určení oblastí, kde k podvodům může docházet. [6]

Nejzávažnější podvody zaměstnanců jsou:

Nadměrně rizikové obchody – není vždy jednoznačné, do jaké míry je riziko ještě přijatelné a od kdy je již nadměrné. Většinou o tom musí rozhodnout až soud. Rizikové obchody bankovních domů byly jednou z příčin celosvětové finanční krize roku 2008. Evropská unie (EU) tak navrhuje v nové Strukturální reformě bankovního sektoru EU omezit svobodu největších bank realizovat nejrůznější typy spekulativního obchodování.[8]

Majetková zpronevěra – všude, kde mají zaměstnanci přímý přístup k majetku nebo financím firmy, je riziko majetkové zpronevěry. Podvody tohoto typu nelákají pouze řadové zaměstnance, ale v řadě případů i vyšší a někdy dokonce i top management. Každá větší organizace je tak nucena průběžně investovat do kontrolních mechanismů a monitorování aktivit svých zaměstnanců.

Korupce – je obecně známa jako zneužití určitého postavení nebo moci k osobnímu prospěchu v tomto případě zaměstnance. Zde je opět zapotřebí sofistikovaných kontrolních mechanizmů uvnitř organizace a také transparentnost veškerých rozhodnutí ovlivnitelných osob.

Falšování finančních výkazů – podvodná jednání tohoto typu se nevztahují pouze na jednotlivce, ale také na celá finanční oddělení potažmo top management velkých společností. Snaha o zkreslování výsledků firmy je zapříčiněna především z důvodu lepší reputace a bonity v očích obchodních partnerů, bank, akcionářů i veřejnosti. Jako nejznámější příklady tohoto jednání můžeme považovat firmy Enron, Olympus nebo WorldCom.

Mezi další časté podvody páchané zaměstnanci patří:

- podvody při fakturaci,

- neoprávněné proplácení výdajů poskytovaných zaměstnanci v souvislosti s výkonem práce,
- nezaúčtování tržeb,
- neoprávněné výplaty zaměstnanců (černé duše, prémie, kompenzace),
- používání firemních prostředků na soukromé účely.

1.3 Podvody pachatelů zvenčí

Jedná se o podvody osob nebo organizovaných skupin, kterými se snaží pachatelé například podvodně vylákat finance z bank nebo ostatních subjektů. Cílem těchto podvodů může být pozměnění nebo padělání listin, ovlivnění zaměstnanců poškozené společnosti nebo provedení pojišťovacího podvodu. Tak jak se vyvíjejí nové technologie a komunikační kanály s klienty, vyvíjí se i podoba těchto podvodných jednání a rozrůstá se i teritorium, na kterém jsou podvodníci schopni operovat.

Pojistné podvody – asi nejlépe definuje pojistný podvod přímo ustanovení §210 trestního zákona o trestném činu pojistného podvodu, které ve svém prvním odstavci uvádí, že kdo uvede nepravdivé nebo hrubě zkreslené údaje nebo podstatné údaje zamlčí v souvislosti s uzavíráním nebo změnou pojistné smlouvy, či v souvislosti s likvidací pojistné události, nebo při uplatnění práva na plnění z pojištění nebo jiné obdobné plnění. (Zákon č. 40/2009 Sb. Trestní zákon)

Falešné směnky či bankovní záruky - zde můžeme uvést například nechvalně známé zástavy „drahých“ kamenů v 90. letech, na základě kterých banky vydávaly záruky nebo přímo úvěry. Tyto kameny ale neměly v podstatě žádnou hodnotu a posudky na jejich cenu byly značně nadsazené. Začátkem 90. let byl tento podvod velice rozšířen a téměř všechny Československé banky s ním měly zkušenost. Po provalení principu celého podvodu přestaly finanční ústavy přijímat drahé kameny jako záruku. Bylo však již pozdě a celý bankovní trh jen v České republice prodělal na těchto obchodech téměř 20 miliard korun.

Podvody s cennými papíry – jedná se o podvody nebo klamavé praktiky nejčastěji na akciových nebo komoditních trzích. Většinou jde o nákup nebo prodej cenných papírů investorům na základě nepravdivých informací, což často vede ke ztrátám. V České republice je nechvalně znám případ Harvardských fondů podnikatele Viktora Koženého. Ten vylákal

z klientů kupónové privatizace jejich podílové knížky za příslib desetinásobku. Následně však došlo k tunelování fondu prostřednictvím společností se sídlem na Kypru a dále k úpadku fondu. Oba čelní představitelé byli u soudu odsouzeni v nepřítomnosti.

Podvody s investováním – jedná se o přesvědčení subjektu nebo klienta k investici finančních prostředků na základě lživých nebo zkreslených informací.

Speciální typy podvodných jednání:

- **počítačové podvody –** provedení podvodu prostřednictvím informační technologie,
- **praní špinavých peněz a financování terorismu –** proces přeměnění peněz z nelegální činnosti na peníze legální,
- **fiktivní bankovní domy –** využití pozměněného nebo fiktivního jména banky a působení bez licence.

1.4 Definice fraud managementu

Fraud management je v dnešní době velmi často používaný výraz. Jedná se v podstatě o ekvivalent poněkud těžkopádného českého výrazu pro řízení rizika podvodů. Nedílnou součástí tohoto řízení je také zabezpečení předcházení těmto podvodům především ve finančních institucích. Podvodným jednáním v tomto případě asociujeme nejrůznější pokusy a činnosti vedoucí k nenásilnému obohacení jako jsou krádež, korupce, zpronevěra, vydírání a v neposlední řadě také praní špinavých peněz a financování terorismu. Pokud se na podvod podíváme z právního hlediska, je v České republice definován v trestním zákoníku. Bráno pohledem fraud managementu je však podvod chápán jako podstatně širší pojem a není tedy brán striktně jen jako jeho definice v právním řádu. [6]

2 Základní oblasti bankovních podvodů

Bankovní podvody můžeme rozdělit dle jednotlivých druhů platebního styku.

2.1 Hotovostní platební styk

Historicky se jedná o jeden z tradičních platebních nástrojů, který je stále využíván nejčastěji. Forma hotovostní úhrady představuje pro mnoho lidí stále nejvíce běžnou a jistou formu placení za zboží nebo služby. Bankovky a mince jsou vydávány Českou národní bankou, která se tak stará o jejich emisi, následné třídění a likvidaci poškozených kusů. Hotovostní peníze jsou distribuovány prostřednictvím sítě komerčních bank. Klienti bank mohou provádět vklady a výběry na pobočkách a v síti bankomatů na celém území České republiky. Současná podoba bankovek a mincí vznikla po rozpadu Československa v roce 1993. Bankovky tak obsahují množství ochranných prvků, které již odpovídají evropským standardům. Bankovky jsou v současné době vydávány v sedmi nominálních hodnotách: 20 Kč, 100 Kč, 200 Kč, 500 Kč, 1.000 Kč, 2.000 Kč a 5.000 Kč, mince v šesti 1 Kč, 2 Kč, 5 Kč, 10 Kč, 20 Kč a 50 Kč. Pokusy o podvody s hotovostními platidly mají většinou formu jejich napodobování, případně pozměňování za účelem navýšení jejich hodnoty. Tak jak kurz České koruny roste, dochází i k jejímu častějšímu falšování. Nejčastěji napodobovanými druhy bankovek jsou ty v tisícových hodnotách. Oblíbená je zejména 1.000 Kč bankovka, kde dochází k jejímu častému využití a není tedy tolik nápadná jako hodnota vyšší. Dále jsou na našem území rozšířené podvody s cizí měnou, zejména Americké dolary (dále jen USD) a Euro (dále jen EUR). Při řešení nálezu falešných bankovek nebo mincí jsou kompetentní orgány činné v trestním řízení. Česká národní banka vydala pro účely předcházení těmto podvodům prospekty, na kterých uvádí potřebné poznávací znaky a parametry pro ověření pravosti platidel. [10]

2.2 Bezhotovostní tuzemský platební styk

Nejvíce využívanými druhy bezhotovostního platebního styku jsou:

Kreditní operace - neboli běžné úhrady.

Inkasní úhrady – přímé debetní platby.

Platební karty – speciální typ elektronického platidla (samostatně je popsán níže).

Forma bezhotovostního platebního styku je nejčastěji převod peněz z účtu plátce na účet příjemce. Tato operace předpokládá u obou stran vlastnictví účtu na základě smluvního vztahu s bankou. Banky jsou tak výhradními subjekty zajišťujícími bezhotovostní platební styk. Jde tedy o platby, které probíhají prostřednictvím elektronických převodů finančních prostředků bez nutnosti fyzického převodu peněz mezi jednotlivými účty klientů. [7] V České republice je pro převody mezi bankami vytvořen od roku 1992 systém "**Czech Express Real Time Interbank Gross Settlement** systém" (dále jen CERTIS).

2.3 Systém CERTIS a oversight

Česká národní banka (ČNB) provozuje **jednotné zúčtovací centrum** pro oblast bankovního trhu v České republice s názvem CERTIS.

Jak na svých internetových stánkách ČNB (www.cnb.cz) uvádí, systém CERTIS zpracovává následující transakce: úhrady, inkasa, opravné zúčtování (storna úhrad), transakce přidružených systémů a informační a kontrolní položky. Kdy je každý účastník systému CERTIS **jednoznačně identifikován kódem banky**, jež je povinnou součástí každé bankovní transakce. V rámci platebního styku se používají další číselné kódy (tzv. symboly plateb), které blíže specifikují platbu.

Vznik a provozování systému CERTIS, stejně jako práva a povinnosti účastníků, jsou stanoveny zákonem o platebním styku. Účty pro mezibankovní platební styk jsou vedeny v ČNB na základě smluv o účtech uzavřených s účastníky podle Obchodního zákoníku. Tyto smlouvy stanoví pro všechny účastníky jednotné standardy i právní a technické podmínky pro vedení účtů a pro předávání a zpracování dat mezibankovního platebního styku. [14]

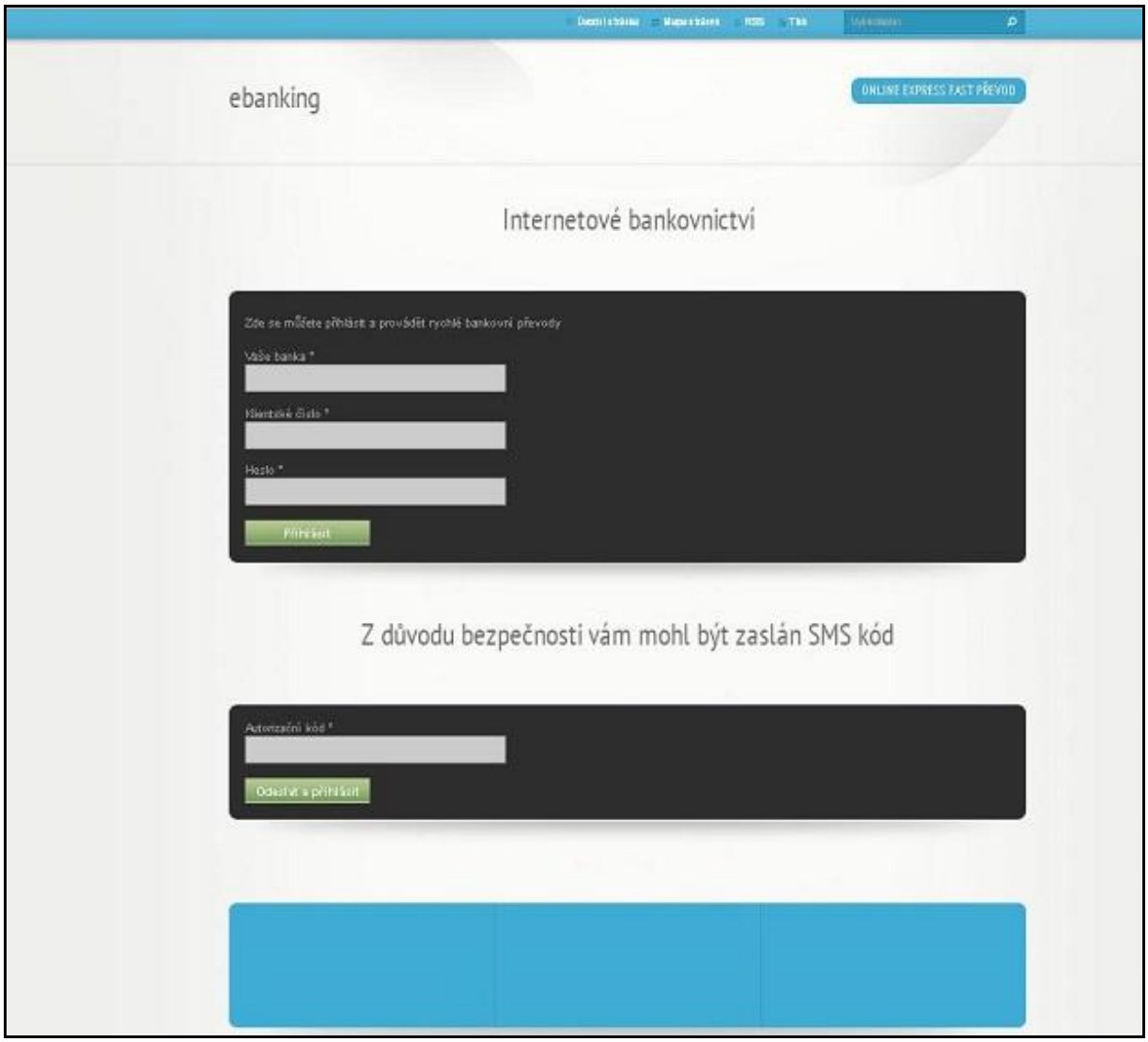
Současně ČNB provádí **dozor** nad platebními systémy, takzvaný **oversight**. Tento systém dozoru se řadí mezi základní funkce Evropského systému centrálních bank a vyplývá ze Smlouvy o založení Evropského Společenství. Oversight je důležitý z hlediska systémového předcházení rizika. Zaměřuje se primárně na platební systémy, neboť představují velký pohyb peněz. V současnosti jsou pod dozorem jak systémy velkých plateb, které jsou významné co do objemu toku financí, tak i systémy malých plateb, které naopak představují velké množství příkazů s malými částkami. Systémem oversight jsou sledovány i kanály pro vypořádání cenných papírů. [13]

2.4 Phishing

V návaznosti na bezhotovostní platební styk je důležité zmínit i způsoby jeho zneužití a možné podvodné jednání. Jako nejčastější způsob zneužití elektronického platebního příkazu je forma takzvaného phishingu. Zjednodušeně se jedná o způsob jak z klientů bank vylákat jejich přístupová hesla a další citlivé informace. Jde o vcelku primitivní, ale účinné podvodné jednání ze stran jednotlivců nebo organizovaných skupin. Slovo phishing vzniklo nejspíše úpravou anglického *fishing*, tedy rybaření. Jako rybář si totiž počíná i útočník, který rozhodí svojí návnadu v podobě falešných e-mailových zpráv nebo webových stránek a poté již jen čeká až se některý z klientů „uloví“. Princip podvodu je tedy založen nejčastěji na elektronických zprávách, které se tváří například jako běžné bankovní oznámení, či výzva klientovi anebo přímo podsouvá falešnou webovou stránku banky. Pokud klient nevěnuje dostatečnou pozornost veškeré své korespondenci a činnosti na internetu a vyplní tento falešný formulář, pak předává veškeré údaje přímo útočníkovi. Ten následně využívá těchto informací k vlastnímu obohacení pomocí správy klientova účtu, nebo informace prodává dále. V dnešní době jsou již zaznamenány i phishingové útoky pomocí sociálních sítí. Princip je stále stejný, jen forma phishingu se neustále vyvíjí, zdokonaluje a přizpůsobuje nejnovějším trendům. [2]

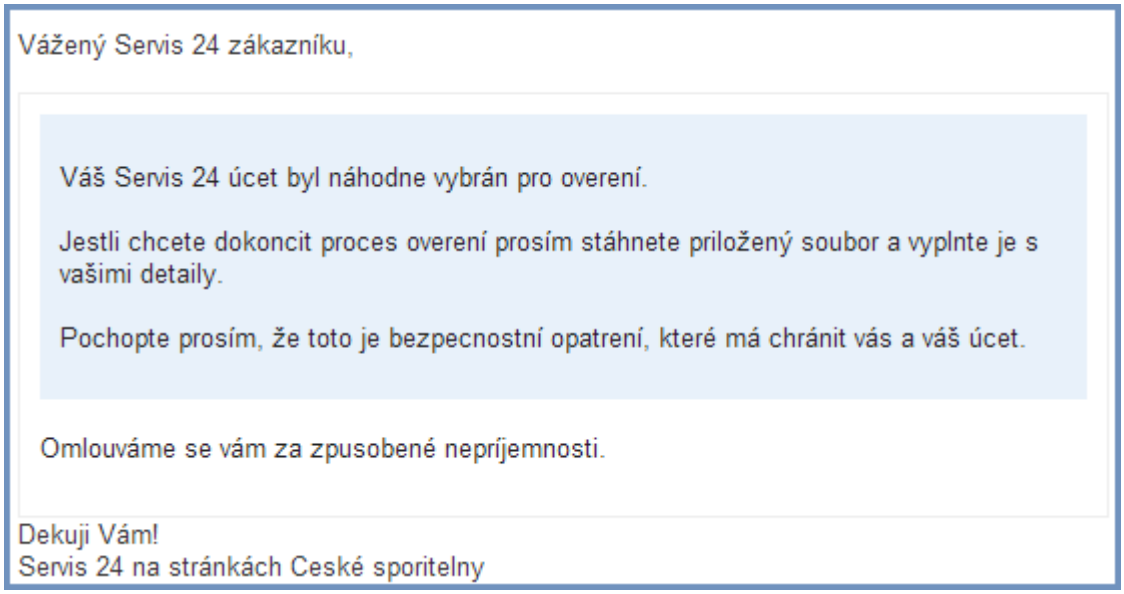
V České republice došlo již k mnoha phishingovým útokům na klienty převážně bankovních institucí, ale například i České pošty. Jeden z příkladů podvodných webových stránek je vidět na obrázku č. 2. Jedná se o pokus zneužití prostřednictvím sociální sítě Facebook. Na obrázku č. 3 je pak názorná ukázka phishingu ve formě e-mailové zprávy rozesílané klientům České Spořitelny.

Obr. č. 2: Phishingová stránka



Zdroj: http://www.csas.cz/banka/nav/o-nas/phishing-d00014536, 2014

Obr. č. 3: Podvodný e-mail



Zdroj: http://www.csas.cz/banka/nav/o-nas/phishing-d00014536, 2014

V oblasti prevence, odhalování a výzkumu phishingu se angažují mnohé státní i nestátní organizace po celém světě. Jednou z nejvýznamnějších je **Anti-Phishing Working Group** (dále jen APWG). APWG byla založena roku 2003 v San Franciscu a je nezávislou neziskovou organizací. APWG průběžně shromažďuje informace a monitoruje phishingové útoky ve světě a pravidelně vydává reporty a informace o boji proti kyber[1] kriminalitě.

Následující tabulka číslo 1 vydaná organizací APWG, zobrazuje počty phishingových útoků celosvětově za 3. kvartál roku 2013.

[1] Kyber – virtuální, počítačový svět

Tab. č. 1: Statistika phishingových útoků za 3. čtvrtletí roku 2013

	Červenec	Srpen	Září
Počet detekovaných podvodných webových stránek	49 480	48 758	45 115
Počet podvodných e-mailových zpráv reportovaných organizaci APWG	61 453	61 792	56 767
Počet společností, proti kterým útok mířil	390	400	379

Zdroj: http://docs.apwg.org/reports/apwg_trends_report_q3_2013.pdf, 2014

2.5 Bezhotovostní zahraniční platební styk a přeshraniční platební styk

Je definován jako provádění platebních příkazů, které lze vymezit jako příkazy k úhradě finančních prostředků:

- platbou do zahraničí ve všech Bankou akceptovatelných měnách,
- platbou ze zahraničí ve všech Bankou akceptovatelných měnách,
- platbou v cizí měně v rámci ČR,
- převodem v rámci Banky v cizích měnách nebo konverzní,
- platbou v CZK v rámci ČR, pokud alespoň jeden z účtů je veden v cizí měně.

Banka při provádění platebního styku musí vždy postupovat v souladu s obecně závaznými právními předpisy, obchodními zvyklostmi a postupy bank v České republice a zásadami stanovenými ČNB.

Základním produktem zahraničního platebního styku je standardní zahraniční platba dle definice výše, která může být, při splnění dalších podmínek testovaných v transakčních aplikacích, zpracována jako SEPA nebo Europlatba (viz níže). Za zahraniční platbu je považována i konverzní platba v rámci účtů jednoho klienta.

SEPA platba je platba v měně EUR, která je především technicky zpracovávána odlišným způsobem od standardní zahraniční platby. Dále rozlišujeme SEPA inkaso, jakožto

bezhotovostní platbu v měně EUR iniciovanou elektronicky z podnětu příjemce prostřednictvím banky příjemce na základě předcházející dohody s plátcem (tzv. mandát).

Standardní zahraniční platba je při zpracování vyslána do banky příjemce ve formátu SWIFT[2] nebo SEPA. Pokud zahraniční platba splňuje podmínky pro zpracování jako Europlatba, je tímto způsobem zpracována a také zpoplatněna. Pokud se jedná o klientské korunové převody v tuzemsku z cizo-měnových účtů, pak je platba zpracovávána konverzním způsobem a dále zaslána do systému tuzemského platebního styku a zpracována jako tuzemská platba.

Převody mezi dvěma účty v rámci jedné banky se provádějí ještě týž den a převod je zpoplatněn buď k tíži plátce (OUR) nebo příjemce (BEN) bez ohledu, zda se jedná o převod mezi účty jednoho nebo dvou klientů podle zadání na platebním příkazu. Papírový platební příkaz znějící na budoucí datum splatnosti je evidován v bankovním systému a zadán v den splatnosti platby. Aktuální disponibilní zůstatek na účtu klienta není dotčen ani elektronicky podaným platebním příkazem s budoucí splatností. Platba se zadává pomocí formuláře určeného pro zahraniční platební příkaz a to papírově nebo elektronicky. Pomocí stejného formuláře lze zadat i příkaz ke konverzi. Na zahraničním platebním příkazu musí být uvedena vždy právě jedna instrukce k platbě. Pro detailní popis zadání zahraničního platebního a trvalého příkazu prostřednictvím kanálů přímého nebo elektronického bankovnictví jsou pro každý z nich k dispozici příručky provádění elektronického platebního styku.

2.6 Europlatba

V zemích Evropského hospodářského prostoru (dále jen EHP) je možné poukázat přeshraniční úhradu prostřednictvím vypořádacího systému STEP2[3] za přesně stanovených pravidel. Europlatba je přeshraniční platba v měně EUR do výše 50.000 EUR.

Aby platba mohla být poukázána jako Europlatba, musí platební příkaz:

- neobsahovat žádný požadavek na zvláštní způsob zpracování,

[2] **SWIFT (Society for Worldwide Interbank Financial Telecommunication)** – Společnost pro celosvětovou mezibankovní finanční telekomunikaci.

[3] **STEP2** – je evropský platební systém umožňující zpracování přeshraničních plateb (do výše 50.000 EUR) v Evropské unii rychleji a levněji než v případě klasického zahraničního platebního styku

- obsahovat správně zadaný IBAN[4] příjemce,
- obsahovat správně zadaný BIC[5] banky příjemce,
- být poplatkována řízením poplatků "SHA".

Pokud v platebním příkazu není dodržena alespoň jedna z výše uvedených povinných náležitostí, nejedná se o Europlatbu, ale o standardní zahraniční platební příkaz a tak je i zpracován a zpoplatněn. V případě, že se jedná o platbu směrovanou do země Evropské měnové unie, příjemce hradí poplatek ve výši standardního poplatku za došlou tuzemskou platbu v dané zemi a platba je mu připsána valutou shodnou s valutou zpracování bankou příjemce. Europlatba může být bance doručena i na papírovém nosiči. V takovém případě bývá k poplatku za Europlatbu navíc připočten speciální příplatek za manuální zpracování.

2.7 SEPA platby

SEPA je zkratka anglického názvu **Single Euro Payments Area**. Základní idea tohoto projektu je zřídit oblast, kde občané, podniky a další hospodářské subjekty budou moci provádět a přijímat platby **v měně EUR v rámci Evropské unie**, ať už přes nebo uvnitř státních hranic za stejných základních podmínek, práv a povinností, bez ohledu na jejich umístění. To vyžaduje odstranění technických, právních a obchodních překážek a následně umožňuje jednotný "domácí" trh plateb v celé evropské zóně a tím i výrazné zlepšení obchodu v eurozóně. Tento projekt vznikl v roce 2008 a klade si za cíl skoncovat s roztříštěností národních platebních systémů a tak od roku 2010 zavádí jednotné evropské platební nástroje. Retailové EUR platby se tak provádí snadno, efektivně a bezpečně po celé Evropě jako v rámci národních hranic. [15]

SEPA platba (SEPA Credit Transfer) je bezhotovostní převod v měně EUR v rámci zemí EHP a Švýcarska, mezi bankami, které přistoupily k systému SEPA, který je standardizován a procesován jednotným evropským clearingovým centrem EBA (European Banking association), nikoliv prostřednictvím SWIFT.

Platební příkaz je vždy zadáván jako SEPA platební příkaz, zadání je tedy odlišné od Europlatby. V přímém a elektronickém bankovnictví je možné tuto platbu zadat

[4] **IBAN - (International Bank Account Number)** – je mezinárodní jednoznačný identifikátor bankovních účtů v příslušné finanční instituci v dané zemi, vyvinutý pro zjednodušení zahraničního platebního styku.
[5] **BIC (Bank Identifier Code, swiftová adresa)** – mezinárodní bankovní kód, 8mi nebo 11ti místný alfanumerický kód jednoznačně identifikující banku nebo její pobočku.

prostřednictvím zvláštní obrazovky, téměř identické a se stejnými povinnými náležitostmi jako pro standardní zahraniční platbu.

Nutné podmínky pro zadání SEPA platby jsou:

- číslo účtu příjemce musí být zadáno ve formátu IBAN,
- banka příjemce identifikována platným BIC kódem,
- banka příjemce je účastníkem systému SEPA, tedy přistoupila k podmínkám zpracovávání SEPA plateb,
- poplatky se aplikují děleným systém (SHA), tedy příjemce i plátce si hradí poplatky u svých bank,
- platba je vždy prováděna v měně EUR, je možné je zaslat i přijmout na účty vedené v jiných měnách, nicméně jsou vždy prováděny konverze do a z EUR.

Zadání SEPA platebního příkazu je možné pouze prostřednictvím přímého nebo elektronického bankovnictví. SEPA platbu nelze realizovat jako platbu trvalého charakteru. SEPA platby není možné podat na papírovém formuláři. SEPA platba se řídí dle SEPA pravidel (tzv. SEPA Rulebook) a nevztahují se na ni případné zvláštní podmínky valutace zahraničních plateb či Europlateb.

SEPA inkaso (SEPA Direct debit) je platba v měně EUR iniciovaná z podnětu příjemce a je prováděna v rámci států EHP a Švýcarska, mezi bankami, které přistoupily k SEPA inkasu. Banka zpracovává oba typy SEPA inkasa:

- **Spotřebitelské SEPA inkaso (CORE)** - je určeno jak spotřebitelům, tak i podnikatelským subjektům. Plátce je oprávněn požádat o vrácení peněžních prostředků (takzvaný refund).
- **Podnikatelské SEPA inkaso (B2B)** – je určeno výhradně podnikatelským subjektům. Jedná se o neodvolatelný typ inkasa, který je podmíněný jednoznačným souhlasem se SEPA inkasem. Proto plátce není oprávněn požádat o vrácení peněžních prostředků (refund).

Klient, který chce vysílat příkazy k SEPA inkasu, musí mít s bankou uzavřenu smlouvu na tuto službu.

3 Podvody v oblasti platebních karet

3.1 Skimming

Jedná se o jednu z nejrozšířenějších forem zneužití platebních karet. Obecně se snaží útočník získat data z platební karty poškozeného a ty zneužít k výběru finančních prostředků z jeho účtu. Jde tedy přímo o klonování dat, které se na platební kartě uchovávají v záznamu na magnetickém proužku, nebo v případě modernějších verzí, v čipu. Padělatelé karet se také v rámci skimmingu snaží získat PIN kód, který je nutný k výběru hotovosti v bankomatech. Skimmovací techniky a zařízení procházejí neustálým vývojem a je prakticky nemožné se všem účinně bránit. Banky a finanční instituce neustále zdokonalují svoje bezpečnostní systémy a bankomaty avšak padělatelé nacházejí stále nové způsoby, jak data ke kartám svých obětí získat. Nedílnou součástí obrany proti skimmingu tak musí být i osvěta a obezřetnost uživatelů platebních karet. [18]

Nejčastěji se se skimmingem setkáváme:

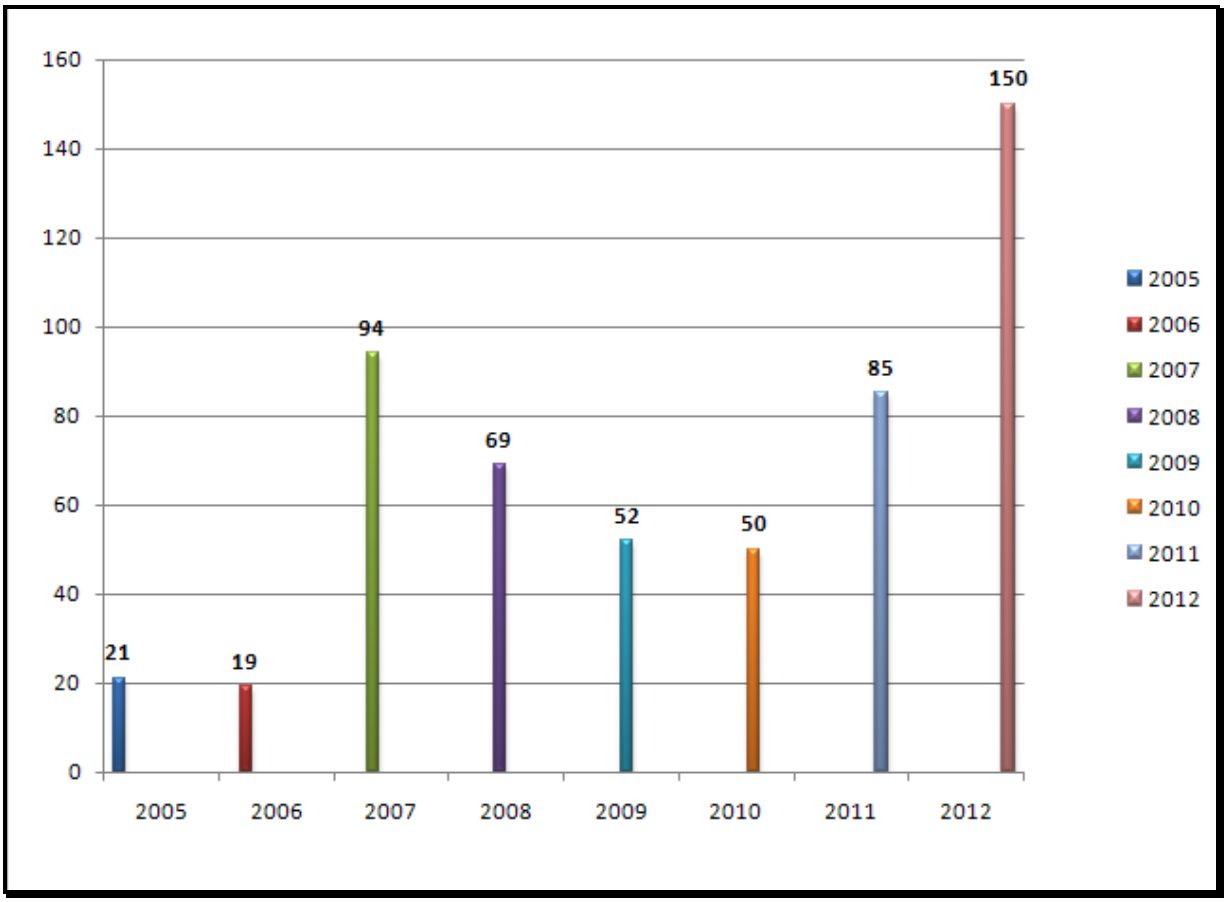
- **U bankomatů** – pachatelé nainstalují kopírovací zařízení přímo na bankomat tak, aby nebylo rozeznatelné od normálního zařízení. Jejich snahou je získat data přímo z karty a také odpozorovat PIN kód jejich potencionální oběti.
- **U obchodníků** – dochází ke zkopírování dat z karty přímo obsluhou daného podniku v době, kdy nemá zákazník kartu přímo pod kontrolou.

3.2 Jak se skimmingu bránit?

Důležitým faktorem obrany je celková obezřetnost při manipulaci a užívání karty. Každý by měl mít svoji kartu neustále pod kontrolou, nikdy ji neponechávat k manipulaci někým jiným. Dále je nutné uchovávat v tajnosti PIN kód. Nesdělovat ho ani svým blízkým, nepřenášet ho v peněžence nebo v blízkosti karty. V případě zadávání kódu na klávesnici bankomatu nebo u obchodníků je důležité mít zakryté ruce tak, aby nebylo možné PIN odpozorovat. Před provedením výběru u bankomatu je také nutné přesvědčit se, že není nestandardně upraven a při sebemenším podezření výběr provést na jiném místě. Pokud již dojde ke ztrátě karty, nebo je podezření, že karta byla skimmována, je nezbytné kartu co nejdříve zablokovat. Dobrým nástrojem k prevenci zneužití je také správné nastavení limitů denních a celkových výběrů. V neposlední řadě je důležité kontrolovat výpisy z účtu

a mít tak celkový přehled o pohybu peněz. I v případě, že se uživatel karty stal obětí této pasti, nemusí to pro něj znamenat finanční újmu. Banky své klienty proti skimmingu chrání a pokud se podaří případ odhalit, většinou ukradené prostředky na účet podvedeného vrátí a sami pak nárokují po padělatelích.

Obr. č. 4: Přehled počtu skimmování na území ČR 2005-2012



Zdroj: http://www.policie.cz/clanek/skimming-2011.aspx, 2014

3.3 Libanonská smyčka

Jde o velice jednoduchý, avšak důmyslný způsob jak získat přístup k platební kartě klienta banky. Útok se odehrává přímo u bankomatu. Princip je založen na smyčce, která je vyrobena nejčastěji z magnetofonového pásku. Ten se připevní na štěrbinu, kterou se vkládá karta do bankomatu. Útočníci nastraží tuto past a čekají na klienta, který chce uskutečnit výběr. Po vložení karty dojde k jejímu nepřečtení, nebo chybnému načtení. Bankomat tak ohlásí chybu, nebo nereaguje vůbec. Podvodníci spolu se smyčkou umisťují na zařízení i falešné číslo infolinky technické podpory. Pokud na něj klient následně zavolá, je požádán o sdělení

PIN kódu. Případně se mohou útočníci tvářit jako obsluha bankomatu a i v tomto případě je jejich hlavní snahou vylákání PIN kódu. V případě, že je uživatel karty obelhán a svůj PIN kód těmto osobám sdělí, mají útočníci možnost bezprostředně po tomto triku uskutečnit z karty výběr.

Libanonská smyčka dostala svůj název od gangů z Libanonu, které ji hojně využívaly. Dnes je již tato metoda velmi známá, a tak je její využití spíše sporadické. To je dáno i novými způsoby zabezpečení bankomatů takzvanými antiskimmovacími nástavci na vstupním otvoru pro karty. Jde tak spíše o ukázkový příklad obelhání klientů, na kterém je názorně vidět vynalézavost podvodníků a je důležité si z něj vzít ponaučení, že i jednoduché podvodné triky mohou být velice úspěšné.

Obr. č. 5: Libanonská smyčka

Zdroj: http://www.atmscams.com/Lebanese%20Loop.html, 2014

3.4 Shimming

Jedna z nejnovějších technik podvodníků jak se dostat k údajům z platebních karet v bankomatu. Jedná se o ultra tenkou destičku (tenčí než lidský vlas) s elektronickým

obvodem a čipem, kterou podvodníci zavedou do slotu pro čtení karty v bankomatu. Destička obsahuje čtecí zařízení a zároveň je zde schopnost odeslat získaná data na vzdálený mobilní telefon nebo tablet pomocí bezdrátového přenosu. Tato technika je vysoce moderní a stále ještě ve stádiu vývoje, nicméně již jsou známy pokusy o její využití. Výrobci bankomatů se snaží těmto pokusům předcházet pomocí zavedení šifrované komunikace mezi čipem karty a snímačem bankomatu. [16]

3.5 Shoulder surfing

Jednoduchá technika kdy se útoční snaží přes rameno oběti zjistit její kód PIN. Následně se snaží podvodník odvrátit pozornost a dostat se tak k platební kartě. Častým způsobem bývá upozornění dotyčného, že mu upadla nějaká bankovka. Jakmile se pro bankovku, nastraženou lupiči, sehne, je mu karta z bankomatu druhou osobou ukradena. Ačkoliv jde o velmi známý a primitivní způsob získání platební karty, stále se najdou jedinci, kteří mu podlehnou. Důležité je v tomto případě zachovat klid a v případě zjištění krádeže okamžitě kartu zablokovat. [17]

4 Související legislativa v České republice

Cílem této práce není popis legislativních skutečností ani není právnickým dokumentem. Obsah této kapitoly má tak za úkol především nastínit oblasti a příslušné zákony, které se problematikou podvodů v bankovní a finanční sféře zabývají a řeší případné následky podvodných jednání.

Se vstupem České republiky do Evropské unie ke dni 01.05.2004 vznikla i nutnost harmonizace českého práva s právem Evropského společenství. Právní požadavky EU se zaměřily i na vylepšení ochrany spotřebitele před podvodným jednáním. Jedním z nových nástrojů, který v této souvislosti vznikl, byl institut finančního arbitra. Ten, jakožto fyzická osoba, může v rozhodování sporů vystupovat jako neutrální třetí strana. Řízení před finančním arbitrem je upraveno zákonem č. 229/2002 Sb., o finančním arbitrovi. [10]

Zákon č. 40/2009 Sb., trestní zákoník, který vstoupil v platnost dne 01.01.2010 zásadním způsobem změnil definování trestného činu. Jeho založení na formálně – materiálním principu bylo změněno na pojetí převážně formální. [19] Dále přinesl i rozšíření své účinnosti na oblast informačních technologií. Ze své podstaty není možné obsáhnout všechny způsoby podvodných jednání a to zejména v oblasti finanční kriminality. Mnoho nových podvodných technik se stále vyvíjí s rozvojem nových služeb v oblasti informačních technologií i na poli platebních karet. V trestním zákoníku však najdeme řadu kategorií, pod které lze většinu podvodů zahrnout. Nalezneme zde základní definici podvodu a podvodných jednání a to v Hlavě V. - Trestné činy proti majetku. Např.:

- § 209 Podvod
- § 210 Pojistný podvod
- § 211 Úvěrový podvod
- § 216 Legalizace výnosů z trestné činnosti

Dále jsou obsaženy podvody v oblasti hotovostního platebního styku v Hlavě VI. Např.:

- § 233 Padělání a pozměnění peněz,
- § 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku,
- § 235 Udávání padělaných a pozměněných peněz,

- § 236 Výroba a držení padělatelského náčiní,
- § 237 Neoprávněná výroba peněz.

A jsou zde uvedeny i **podvodná jednání na poli informačních technologií**:

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací,
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

Jako další právní normu je třeba zmínit zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, který podrobněji upravuje například oblast mlčenlivosti, archivace dokumentů a dalších provozních záležitostí. Jedná se svým určením o základní zákon k bankovní problematice.

Dalšími souvisejícími zákony a vyhlášky zabývající se přímo jednotlivými oblastmi finančního trhu jsou:

- **Zákon č. 253/2008 Sb.,** o některých opatřeních **proti legalizaci výnosů z trestné činnosti a financování terorismu.**
- **Vyhláška České národní banky č. 281/2008 Sb.,** ze dne 1. srpna 2008, o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu.
- **Směrnice Evropského parlamentu a Rady 2005/60/ES** ze dne 26. října 2005 o předcházení zneužití finančního systému k praní peněz a financování terorismu.
- **Zákon č. 284/2009, o platebním styku** (který ruší Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech),
- **Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí.**
- **Zákon č. 254/2004 Sb., o omezení plateb v hotovosti**, ve znění pozdějších předpisů.
- **Vyhláška č. 62/2004 Sb**., kterou se stanoví **způsob provádění platebního styku mezi bankami**, zúčtování na účtech u bank a technické postupy bank při opravném zúčtování.

5 UniCredit Bank Czech Republic and Slovakia, a.s.

Nadnárodní skupina UniCredit Group vznikla sloučením devíti velkých italských bank a s následnou integrací s německou skupinou HVB a italskou bankou Capitalia. Skupina UniCredit Group patří podle bilanční sumy ve výši 1,028 bilionu EUR k největším finančním skupinám v Evropě. Působí přímo ve 22 zemích a ve 27 zemích prostřednictvím svých obchodních zastoupení, má přes 40 mil. klientů, přibližně 10 000 poboček a 168 000 zaměstnanců. V regionu střední a východní Evropy disponuje tato skupina největší mezinárodní bankovní sítí, kterou představuje 4 000 poboček a prodejních míst s více než 83 000 zaměstnanců a 28 milióny klientů.

Obr. č. 6: Logo UniCredit Bank

Zdroj: http://www.unicreditbank.cz/web/o-bance/tiskove-centrum/logo, 2014

UniCredit Bank Czech Republic and Slovakia, a.s. (dále jen UniCredit) je součástí skupiny UniCredit Group a zahájila svoji činnost na českém trhu 5. listopadu 2007. Původní **UniCredit Bank,** která působila pouze v České republice, vznikla sloučením dvou dosud samostatně působících úspěšných bankovních domů HVB Bank a Živnostenské banky. Následně došlo koncem roku 2013 k sloučení s UniCredit Bank Slovakia a celý název se tedy rozšířil na **UniCredit Bank Czech Republic and Slovakia, a.s.** Strategie banky je zaměřena na rychlý rozvoj na poli retailového i korporátního finančního trhu. Přední příčky mezi bankami pravidelně obsazuje v oblasti akvizičního financování a financování komerčních nemovitostí. Pobočková síť prochází neustále rychlým rozvojem s důrazem na kvalitu poskytovaných služeb privátní klientele. UniCredit provozuje Evropské kompetenční centrum, prostřednictvím kterého mají zákazníci možnost nabídku služeb pro financování projektů ze strukturálních fondů EU. Dalším specializovaným pracovištěm je Kompetenční centrum, které cílí na svobodná povolání, jakými jsou např.: lékaři, soudci, advokáti, notáři

apod. Silnou pozici také banka zaujímá na trhu privátního bankovnictví, cenných papírů, kreditních karet a hypoték. [22]

Hlavním orgánem banky je představenstvo. Jako předseda představenstva byl jmenován Ing. Jiří Kunert, který je považován za předního českého experta na finančním a bankovním trhu. V oblasti bankovnictví působí již více než 38 let. Výše základního kapitálu banky zapsaného v obchodním rejstříku byl ke dni 14. června 2013 celkem 8.749.716.000 Kč. Organizační struktura banky zahrnuje následující počty organizačních jednotek: 7 divizí, 26 úseků, 38 odborů, 86 oddělení centrály, 6 obchodních oblastí, 21 regionálních center firemní klientely, 10 retailových[6] obchodních regionů a 103 poboček. Celkový stav zaměstnanců banky se pohybuje okolo 1930. [20]

5.1 Nabízené bankovní služby

Banka UniCredit se zaměřuje na širokou škálu bankovních služeb jak pro veřejnost, tak pro korporátní[7] klientelu.

Hlavní činnosti vykonávané na základě bankovní licence jsou:

1. přijímání vkladů od veřejnosti,
2. poskytování úvěrů,
3. investování do cenných papírů na vlastní účet,
4. platební styk a zúčtování,
5. vydávání a správa platebních prostředků,
6. poskytování záruk,
7. otvírání akreditivů,
8. obstarávání inkasa,
9. poskytování investičních služeb,
10. vydávání hypotečních zástavních listů,
11. finanční makléřství,
12. výkon funkce depozitáře,

[6] Retail = maloobchodní prodej
[7] Korporátní = firemní

13. směnárenská činnost (nákup devizových prostředků),
14. poskytování bankovních informací,
15. obchodování na vlastní účet nebo na účet klienta,
16. s devizovými hodnotami a se zlatem,
17. pronájem bezpečnostních schránek.

Jednotlivé **core[8] činnosti banky** jsou rozděleny dle jejich adresátů následovně:

Občané: účty a konta, platební karty, úvěry, hypotéky, vklady a investice, online služby, pojištění.

Svobodná povolání: účty a konta, platební karty, úvěry, vklady a investice, online služby, pojištěni a ostatní služby.

Podnikatelé a menší firmy (roční obrat do 50 mil. Kč): účty a konta, platební karty, úvěry, vklady a investice, online služby, pojištěni a ostatní služby.

Firmy a veřejný sektor (roční obrat nad 50 mil. Kč): zde se banka zaměřuje mimo standardních korporátních služeb na řízení finančních rizik, financování a zajišťování obchodních transakcí a využití a čerpání prostředků z fondů Evropské unie. [21]

5.2 Elektronické kanály

1) Internetové bankovnictví Online Banking

Online Banking je moderní, bezpečný a efektivní způsob řízení financí prostřednictvím internetu 24 hodin 7 dní v týdnu. Pro zabezpečení jsou využívány nejmodernější způsoby, které jsou prověřeny v rámci celé skupiny UniCredit. Online Banking zákazníkům nabízí širokou škálu služeb pro správu jejich bankovního konta. Podmínkou pro poskytnutí internetového bankovnictví je běžný účet v bance UniCredit. Mezi nevyužívanější funkce patří:

- přehled a historii účtů, debetních a kreditních karet a cenných papírů,
- výpisy z účtu ve formátu PDF,

[8] Core = základní činnosti

- zadání, změnu a zrušení trvalých příkazů a termínovaných vkladů,
- nastavení splátky kreditní karty,
- dobíjení předplacených SIM karet mobilních operátorů,
- nastavení zasílání SMS a e-mail informací, např. o zůstatku.

2) Aplikace MultiCash

Jedná se o aplikaci vzdáleného přístupu do banky, kterou v rámci České republiky využívá 15 bank. Je dodávána ve verzích přizpůsobených bankovním standardům většiny evropských a mnoha dalších zemí. Výrobcem je německá firma Omikron Systemhaus GmbH. Komunikace s bankou probíhá prostřednictvím analogové či ISDN telefonní linky nebo internetu (TCP/IP protokol).

Využití této aplikace je výhodné především pro střední a větší korporátní klienty. Prostřednictvím tohoto software jsou klienti banky schopni zpracovávat denně velké množství platebních příkazů, ovládat účty více společností přímo z jedné aplikace, ovládat účty vedené i v jiných českých bankách, ovládat účty vedené i v zahraničních bankách a přijímat výpisy z účtů vedených v jiných bankách. Aplikace MultiCash je tak vhodný nástroj pro účetní oddělení, kde je využíváno množství firemních účtů v různých bankách, které nabízejí jejich správu prostřednictvím MultiCash. [24]

Funkčnosti aplikace MultiCash

- Pořizování tuzemských platebních příkazů (standardní, expresní platby, žádosti o inkaso).
- Pořizování zahraničních platebních příkazů (standardní platba, Europlatba, SEPA platba, SEPA inkaso).
- Načítání a zpracování tuzemských a zahraničních platebních příkazů ze souboru vytvořeného účetním systémem.
- Zobrazení aktuálních zůstatků a historie transakcí.
- Spravování účtů více společností v rámci jednoho uživatelského přístupu.
- Spravování účtů vedených ve více bankách v rámci České republiky.

- Spravování účtů ve více zemích pomocí připojení na zahraniční bankovní server, pomocí SWIFT zpráv nebo aplikace EuropeanGate.
- Flexibilní nastavení podpisových oprávnění na úrovni účtu a uživatele.
- Možnost vytvářet a sdílet s ostatními uživateli šablony platebních příkazů a databáze obchodních partnerů.
- Archiv příkazů – historie autorizovaných (podepsaných) transakcí předaných bance ke zpracování.
- Přístup k elektronickým výpisům z účtů UniCredit Bank, které lze pohodlně importovat do účetnictví.
- Možnost přijímání zpráv zasílaných bankou.
- Správa profilů práv jednotlivých uživatelů.

3) Aplikace Eltrans

Eltrans je multibankovní aplikace vyvinutá českou společností BSC Praha, spol. s r. o. V rámci České republiky produkt využívá šest bank. Tak jako aplikace MultiCash se jedná o prostředek ke správě velkého počtu účtů v různých bankách (podporujících Eltrans) a to prostřednictvím Klient-Server konfigurace s využitím internetového nebo ISDN připojení. [24]

4) Aplikace BusinessNET

BusinessNet je službou internetového bankovnictví vytvořenou s cílem uspokojit náročné potřeby firemních klientů. K obsluze firemních účtů prostřednictvím služby BusinessNet postačí přístup na internet, internetový prohlížeč a na počítači nezávislý mobilní nebo pevný bezpečnostní klíč. Hlavní devizou tohoto přístupu k firemním účtům tak je možnost přístupu odkudkoliv bez nutnosti pevné softwarové instalace. A dále také možnost ovládat své finance vedené v dalších bankách skupiny UniCredit v zahraničí v jediné aplikaci prostřednictvím jediného uživatelského čísla a bezpečnostního klíče. [24]

5.3 Typy zabezpečení elektronických kanálů banky UniCredit proti zneužití

1) Smart klíč

Mobilní aplikace, která generuje **jednorázové, časově omezené kódy**. Majitelé chytrých zařízení mohou získat Smart klíč stažením aplikace Smart Banking z Google Play nebo App Store. Ostatní mobilní telefony (s podporou Java) si stahují separátní aplikaci, jejíž odkaz zasílá banka formou SMS. Výhodami aplikace Smart klíč jsou: aplikace je zdarma, zabezpečení má klient vždy při sobě a nemusí nosit další zařízení, 100% kontrola nad podepisovanými transakcemi, nezávislost na rychlosti doručení bezpečnostního kódu prostřednictvím například SMS. [24]

2) SMS klíč

Kódy pro přihlášení a platby v Online Banking jsou klientovi doručovány **prostřednictvím SMS zpráv** přímo a neprodleně na jeho mobilní telefon. Při zvolení tohoto typu zabezpečení je zapotřebí vyplnit emailovou adresu pro zaslání vstupního bezpečnostního kódu a číslo mobilního telefonu pro zasílání jednorázových SMS kódů. Výhodou SMS klíče je snadné a rychlé použití a doručení přímo na mobilní telefon klienta. Avšak má i svoje nedostatky, kterými je závislost na dostupnosti mobilního signálu a doručení klíče pouze na území České republiky. [24]

3) Bezpečnostní klíč - token

Token je malé elektronické zařízení ve tvaru kalkulačky, které se aktivuje **pomocí vlastního PINu** a je určeno k vygenerování kódu pro přihlášení nebo podpis elektronické platby. Bezpečnostní token je vhodný pro klienty, kteří nechtějí ke své autentizaci a ověřování plateb využívat mobilní telefon. Jeho pořízení je zpoplatněno, následné užívání až do vybití baterie už nikoliv. Jedná se o velmi silnou autentizaci avšak na úkor její praktičnosti. V současné době již tokeny ustupují právě autentizaci pomocí bezpečnostních klíčů v mobilních telefonech a SMS klíčům. [24]

4) Vzdálený podpis

Využití vzdáleného podpisu je především v aplikacích architektury Klient-Server, tedy MultiCash a Eltrans. Jedná se o výměnu privátního klíče **bezpečnostního certifikátu**, který je následně pomocí veřejného klíče ověřen a uložen pro potřebu další komunikace aplikace s bankou. Při každém dalším spojení tak již není nutné podpis ověřovat a ten je vždy až do vypršení platnosti použit. Výměna dat v aplikacích Eltrans a Multicash mezi bankovní a klientskou stranou probíhá přes takzvaný **SSL protokol**, což je transportní šifrovaná vrstva založená právě na výměně veřejného a soukromého šifrovacího klíče. [24]

5.4 Prevence podvodných jednání v rámci UniCredit

Banka UniCredit staví základy fraud managementu na **prevenci**. Ta je nejdůležitějším nástrojem k předcházení ekonomické a reputační škody způsobené spácháním podvodného jednání ať už proti bance, nebo proti jejím klientům. Účinná prevence, která je schopna chránit majetek společnosti je založena na chování každého zaměstnance, které musí být zároveň plně podporováno ze strany vedení. Banka si zejména zakládá na etickém, poctivém a transparentním prostředí a přímo se snaží aktivně působit v typických oblastech **předcházení podvodům**, jakými jsou: hodnocení rizik, lidské zdroje, výzkum a vývoj, informační technologie.

5.5 Hodnocení rizik

Jedním z prvních kroků boje proti podvodům **je určení faktorů rizika podvodu** a jejich velikosti. Je důležité zjistit pravděpodobnost "**modus operandi**"[9] rizika, kdy může dojít k poškození na straně banky a na tomto základě zajistit příslušná preventivní opatření. Jedním z hlavních úkolů je tak zhodnotit a průběžně aktualizovat potencionální riziko v rámci banky a na tomto základě stanovit strategii prevence.

5.6 Lidské zdroje

Školení zúčastněných stran a povědomí o podvodech je dalším základním kamenem prevence a odhalování trestné činnosti. V bance UniCredit je **soustavnou školící činností** zajištěno,

[9]Modus operandi - charakteristická posloupnost činů kriminální činnosti

aby si všichni pracovníci byli vědomi svých povinností pro kontrolu podvodů a etického chování. Přesně cílená školení mají za úkol poskytnout nově přijatým zaměstnancům informace o následujících tématech:

- definice podvodu a jeho vlastnosti,
- potřeba etického chování a skutečnost, že vyhýbání se podvodu je odpovědností každého,
- pravidla UniCredit banky, které zcela nebo částečně řeší témata podvodů,
- ukazatele výskytu podvodu,
- nutné kroky, v případě důvodného podezření ze spáchání podvodu,
- odpovědnost za řízení obvinění a vyšetřování v případech podvodů v rámci banky,
- odpovědné osoby v rámci banky, zodpovědné za fraud management společnosti.

5.7 Výzkum a vývoj

Analýza možných podvodných budoucích scénářů a následné metodické a procesní řešení a nástroje prevence rizik vzniku podvodů jsou **zásadní pro odpovídající prevenci**. To je cílem průběžného výzkumu a vývoje, kterou má na starosti oddělení bezpečnosti.

5.8 Informační technologie

Prevence podvodného jednání, stejně tak jako v případě lidského faktoru, musí být také podporována technologickými prostředky určenými k jeho identifikaci, a pokud je to možné, vedoucí k jeho zabránění. Odpovědní zaměstnanci banky v oblasti IT systémů jsou přímo vedeni k zajištění požadovaného směru a úrovně bezpečnosti ve výpočetních systémech banky. Důraz je třeba zaměřit zejména na následující oblasti:

- zajistit **dostupnost, důvěrnost a integritu** dat a informací,
- dosáhnout a udržet si co **nejvyšší úroveň bezpečnosti** pro všechny technologická zařízení, ať už přímo, nebo nepřímo ve vztahu k provozní bankovní obchodní činnosti,
- zajistit podmínky pro přístup a využití informačních nástrojů s cílem respektovat **zásady bezpečnosti informací**,

- zajistit technologické nástroje potřebné k rozpoznání a identifikaci jakýchkoliv **anomálií** v rámci spravovaného softwarového prostředí a technologické infrastruktury,
- zajistit technologické nástroje potřebné k identifikaci anomálií v bankovních obchodních operacích.

6 Praní špinavých peněz a financování terorismu

Mohlo by se zdát, že se jedná převážně o fenomén poslední doby kdy je **boj proti financování terorismu a praní špinavých peněz** jednou z hlavních bezpečnostních priorit mnoha států západní civilizace. Praní špinavých peněz jako takové má však své kořeny ještě v době největších mafiánských klanů ve 20. a 30. letech dvacátého století. Klany získávaly peníze nelegálním prodejem alkoholu nebo drog a ty se pak snažily vyčistit, tedy zlegalizovat. Princip zůstává stejný, avšak vynalézavost novodobých „mafiánů“ stále roste. [4]

Financování terorismu se řadí v podstatě do stejné kategorie, bývá však z pravidla daleko lépe organizované. Nejen že teroristické organizace prorůstají čím dál více do západních kultur, ale tento způsob získávání finančních prostředků je mnohdy podporován i vládami mnoha zemí. Snaží se tak získat prostředky pro svůj boj, který může mít mnoho podob. Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu přímo říká, že financováním terorismu se rozumí: *„Shromažďování nebo poskytnutí peněžních prostředků nebo jiného majetku s vědomím, že bude, byť jen zčásti, použit ke spáchání trestného činu teroru, teroristického útoku nebo trestného činu, který má umožnit nebo napomoci spáchání takového trestného činu, nebo podpoře osoby nebo skupiny osob připravujících se ke spáchání takového trestného činu, nebo jednání vedoucí k poskytnutí odměny nebo odškodnění pachatele trestného činu teroru, teroristického útoku nebo trestného činu, který má umožnit nebo napomoci spáchání takového trestného činu, nebo osoby pachateli blízké ve smyslu trestního zákona, nebo sbírání prostředků na takovou odměnu nebo na odškodnění.“*

6.1 Procesy praní peněz

1) Namáčení

První etapa procesu praní je nejobtížnější a nejdůležitější fází. Využívá se tzv. **smurfingu** (šmoulování). Jeho podstata je ve využití velkého počtu účtů v různých bankách k vložení hotovosti po malých částkách různými osobami. Tato metoda je stále využívána, ačkoli je poměrně primitivní a organizačně i časově dosti nákladná. Jde však o to, aby bance nevznikla oznamovací povinnost, jak tomu u vyšších částek je, a tedy nevzbudily vklady pozornost. Následně je možné s penězi již dále nakládat v rámci bezhotovostního platebního styku. [23]

2) Mydlení

Provádí se různými technikami a jde zde především o **znemožnění** účetní kontrole **zjistit původní zdroj** peněz. Tato operace je klíčová, jelikož je nutné finance nejen očistit, ale i zlikvidovat stopy po jejich původu. Jsou tak uskutečňovány nejrůznější fingované prodeje v podnicích, které přijímají hotovosti (restaurace, maloobchody s elektronikou, klenotnictví, aj.), případně se uzavírají hypotéky a nejrůznější pojištění, aby se následně opět rychle zrušilo atd. Jsou také využívány různé herny a kasina, kde dochází k náhlým výhrám a dále se provádějí co nejsložitější finanční transakce. [23]

3) Ždímání

Vyprané výnosy se následně **vracejí zpět do finančního systému:** *„Vyprané peníze, které prošly oběma předchozími etapami a zastřely tak svůj původ, se vracejí ve formě nezávadného, legálního a často zdanitelného příjmu původnímu majiteli.“* [23]

6.2 Politika UniCredit banky proti praní peněz a financování terorismu

Banka UniCredit má ve své organizační struktuře útvar, který se přímo specializuje na boj s těmito podvody, jedná se o oddělení AML (z anglického Anti-Money Laundering). Při rozličnosti a složitosti problematiky praní špinavých peněz a financování terorismu můžeme realizovaná opatření banky shrnout do 3 hlavních zásad:

1. **Poznat svého klienta!** Identifikační údaje a informace zjištěné při kontrole klienta jsou zaznamenávané do informačního systému banky. Při pochybnostech si pracovník je povinen vyžádat dokumenty, které potvrdí důvěryhodnost klientových sdělení, tyto dokumenty se následně zakládají do archivu.
2. **Udržovat s klientem trvalý obchodní vztah**, aby zaměstnanci poboček rozuměli jím požadovaným službám a obchodům a to jak z hlediska obchodního, tak z hlediska rizik. Důležité je i ověření, zda mají klientem požadované operace ekonomické opodstatnění a zhodnocení případného rizika. Zařazení klienta dle míry rizika, zda se může podílet na praní špinavých peněz nebo financování terorismu.
3. **Provádění pravidelného monitoringu** transakcí klienta, průběžně se ověřují veškeré již zjištěné informace, a to ze všech dostupných zdrojů.

4. Jeden z hlavních pilířů prvotní kontroly je postaven na principu, že **konkrétní pracovník**, který obsluhuje klienta**, je často jedinou osobou** v bance schopnou odhalit podezřelý obchod. [24]

6.3 Rozpoznání podezřelého obchodu

Podezřelým obchodem se rozumí obchod provedený za okolností vyvolávajících podezření ze snahy o legalizaci výnosu nebo podezření, že v obchodu užité prostředky jsou určeny k financování terorismu, teroristických činů nebo teroristických organizací. Jako podezřelá transakce přitom může být označena uskutečněná transakce, ale i nakonec neprovedená (pouze zamýšlená) operace.

O podezřelý obchod se jedná zejména v těchto případech:

1. vklady v hotovosti následované jejich okamžitými výběry nebo převody na jiné účty, zejména do zahraničí,
2. případy, kdy počet obratů na účtu během jednoho dne nebo ve dnech následujících neodpovídá obvyklým peněžním operacím klienta,
3. zřizování účtů jedním klientem, jestliže jejich počet je ve zjevném nepoměru k předmětu jeho podnikatelské činnosti nebo jeho majetkovým poměrům, a převody mezi těmito účty,
4. převody majetku, které nemají zjevný ekonomický důvod,
5. objem pohybů na účtech klienta nebo nakládání s majetkem, který zjevně neodpovídá povaze nebo rozsahu klientovy podnikatelské činnosti nebo jeho majetkovým poměrům,
6. bankovní služby a produkty využívané v rozporu s účelem, pro který byly zřízeny,
7. činnosti, které mohou napomoci klientovi zastřít jeho totožnost, nebo totožnost skutečného majitele,
8. transakce z a do státu, který nedostatečně nebo vůbec neuplatňuje opatření proti legalizaci výnosů z trestné činnosti a financování terorismu,
9. situace, kdy má banka pochybnosti o pravosti získaných identifikačních údajů nebo podkladů pro kontrolu klienta,

10. klientem nebo skutečným majitelem je osoba, vůči níž Česká republika uplatňuje mezinárodní sankce podle zákona č. 69/2006 Sb. o provádění mezinárodních sankcí,
11. předmětem obchodu je nebo má být zboží nebo služby, vůči nimž Česká republika uplatňuje sankce podle zákona č. 69/2006 Sb. o provádění mezinárodních sankcí,
12. klient se odmítá podrobit identifikaci nebo kontrole, nebo odmítá sdělit, za koho jedná. [24]

6.4 Zásada „Poznej svého klienta“

Identifikace a princip KnowYourCustomer (dále jen KYC) = Poznej svého klienta je jedním z hlavních pilířů preventivního odhalování podezřelých obchodů.

Politika KYC sestává ze zjištění rizikových faktorů, kontroly klienta, vyhodnocení a kategorizace z pohledu rizika praní špinavých peněz a financování terorismu. Celý tento proces musí být dokladovatelný a musí být proveden před uskutečněním prvního obchodu a dále dle pravidel KYC v průběhu jeho trvání.

Součástí principů KYC je i politika přijatelnosti klienta (dále jen PPK - viz níže). Povinností každého zaměstnance je dodržování zásad KYC při každé činnosti, která se týká poskytování služeb klientům, jednorázovým klientům nebo dalším obchodním partnerům.

Za aplikaci politik KYC a PPK vůči jednotlivým klientům odpovídá patřičný útvar, odbor nebo pobočka, která zastupuje banku a vstupuje tak s klientem do obchodního vztahu. Hodnocení transakcí podle politiky KYC neznamená, že takový obchod je vyňat z povinnosti ohlásit jej jako podezřelý na FAÚ MF ČR. Pokud zaměstnanec banky UniCredit vyhodnotí, že může jít o podezřelý obchod v souvislosti s problematikou legalizace výnosů z trestné činnosti, postupuje dále dle předpisu pro opatření proti legalizaci výnosů z trestné činnosti a financování terorismu.

KYC je zároveň pro banku i důležitý prodejní nástroj, protože jen s klienty, které jako poskytovatel služeb dobře zná, může navázat dlouhodobý, vzájemně důvěryhodný a trvale uspokojivý obchodní vztah.

Informace získávané od klientů v rámci principu KYC slouží k posouzení jeho aktivit a ekonomické situace a zázemí, důvodu a účelu sjednání obchodního vztahu s bankou, k určení rizikových faktorů klienta a rozpoznání operací, které jsou vzhledem k deklarovaným činnostem klienta a udanému účelu používání účtu či jiných bankovních produktů neobvyklé,

případně podezřelé. Získané informace slouží rovněž pro vyhodnocení přijatelnosti klienta podle politiky PPK popsané níže.

Při prvním navázání obchodního vztahu s klientem – fyzickou osobou v retailovém segmentu je nutné požadovat od klienta informace pro provedení základní kontroly klienta, na jejímž základě bude vyhodnocena rizikovost klienta, respektive stanoven jeho rizikový profil a rozhodnuto, zda u něj bude provedena také hloubková kontrola.

U stávajících klientů se základní kontrola doplňuje postupně například pří příležitosti setkání s klientem (změna údajů, změna parametrů poskytovaných produktů, zájem nebo nabídka nových produktů, úvěrové hodnocení atd.). Údaje zjištěné při základní kontrole klienta se evidují v informačním systému banky. [24]

Základní otázky, které si musí zaměstnanec při styku s klientem položit a na které by měl znát odpovědi jsou:

- **Víte, kdo využívá služeb naší banky?**
- **Znáte zamýšlené transakce klienta**, účel jeho vztahu s naší bankou, zdroj jeho financí?
- **Víte, jak vysoké je riziko**, že se konkrétní klient může podílet na praní špinavých peněz?
- **Jsou pro vás obchody klientů transparentní?** Odpovídají obchody klientů tomu, co o svých klientech víte?

Celý proces dotazníku principu **KnowYourCustomer** je vyjádřen následující tabulkou:

Tab. č. 2: KnowYourCustomer

Víte, kdo využívá služeb naší banky a proč?	→	**1.**	**Identifikace klienta**
Znáte zamýšlené a prováděné transakce klienta?	→	**2.**	**Kontrola klienta**
Skutečně znáte svého klienta?	→	**3.**	**Vyhodnocení a kategorizace klienta**
Jsou pro vás jeho obchody transparentní?	→	**4.**	**Monitorování klientů, účtů a transakcí**

Zdroj: vlastní tvorba dle [24], 2014

Vyhodnocení a kategorizace klienta

Na základě údajů, zadaných při kontrole klienta do dotazníku KYC, dojde k vyhodnocení míry rizikovosti klienta a jeho přijatelnosti nebo nepřijatelnosti. Schéma kontroly klienta v KYC dotazníku a váhu jednotlivých rizikových faktorů pro stanovení rizikovosti znázorňuje tabulka číslo 3. Po stanovení úvodní rizikovosti klienta je tato informace zapsána do informačního systému banky, kde je klient označen příslušným statusem. Pravidla stanovení rizikovosti klienta, přidělený status a tomu odpovídající periodicita kontroly jsou popsány níže.

Banka rozlišuje čtyři **základní kategorie klientů**:

a) nízké riziko AML,

b) střední riziko AML,

c) vysoké riziko AML,

d) neakceptovatelné riziko AML.

Tab. č. 3: Kategorizace klienta

kategorie klienta	stručný popis	míra rizika	periodicita kontroly
Nízké riziko AML	*klient byl na základě KYC informací vyhodnocen jako málo rizikový*	malá	1 x 3 roky
Střední riziko AML	*u klienta byl shledán rizikový faktor, nebo nesplnil podmínky nutné pro přidělení nízkého rizika*	střední	1x za rok
Vysoké riziko AML	*klient byl vyhodnocen jako vysoce podezřelý a rizikový*	vysoká	1 x za 6 měsíců
Neakceptovatelné riziko AML	*s těmito klienty banka nemá a nechce mít uzavřený obchodní vztah, v případě, že obchodní vztah existuje, banka od něj odstoupí*	neakceptovatelná	--------

Zdroj: [24]

Politika přijatelnosti klienta (PPK)

S cílem minimalizovat riziko zneužití banky jako nástroje pro legalizaci výnosů z trestné činnosti a financování terorismu a z toho vyplývajících následků a v souladu s Vyhláškou stanovuje banka kritéria pro navazování obchodních vztahů s klienty. Banka nechce a nebude vstupovat do obchodních vztahů s klienty, u kterých není přesvědčena o transparentnosti jejich úmyslů a o čistotě jimi zamýšlených obchodů, případně neposkytne produkt nebo službu, pokud má podezření, že by tento mohl být klientem zneužit k praní špinavých peněz, financování terorismu, podvodu apod. [24]

6.5 Oznámení podezřelého obchodu

V případě zpozorování podezřelého obchodu pak následuje jeho oznámení. Banka UniCredit je dle Zákona č. 253/2008 Sb. povinna prostřednictvím svého představenstva jmenovat pro tento účel skupinu pověřených pracovníků k zajišťování výměny informací s Finančním analytickým útvarem Ministerstva financí ČR a plnění oznamovací povinnosti ve věci zjištěných podezřelých obchodů. Jsou jimi zpravidla pracovníci oddělení AML nebo

compliance[10] a oddělení bankovní bezpečnosti. Momentálně se jedná o pět nominovaných osob, na které se mohou zaměstnanci s podezřelými obchody kdykoliv obrátit.

6.6 Finanční analytický útvar Ministerstva financí ČR

Jedná se odbor Ministerstva financí České republiky, který vznikl 1. července 1996 přímo pro účely boje proti legalizaci výnosů z trestné činnosti a financování terorismu. Tyto úkoly jsou důsledkem přijetí opatření Rady bezpečnosti OSN pro ochranu lidských práv a boje s terorismem. Odbor provádí sběr a analýzu údajů o podezřelých obchodech a zároveň se stará i o rozvoj a dotváření celého systému opatření proti legalizaci výnosů z trestné činnosti včetně návrhů nových zákonů a prováděcích předpisů. V neposlední řadě je v jeho působnosti i spolupráce s mezinárodními organizacemi a orgány Evropské unie v této oblasti. Poskytuje také školení a semináře finančním institucím. [12]

Mezi hlavní úkoly odboru **Finanční analytický útvar Ministerstva financí ČR** (dále jen FAÚ MF ČR) patří:

- **Přijímat a šetřit** oznámené podezřelé obchody (OPO), v případě podezření ze spáchání trestné činnosti podat trestní oznámení.
- **Kontrolovat** finanční instituce, zda plní dané zákonné podmínky v oblasti.
- **Zajišťovat komunikaci** s obdobnými zahraničními institucemi.
- **Spravovat právní agendu** související s problematikou praní špinavých peněz.

V případě podezření, že klientem požadovaný nebo realizovaný obchod lze hodnotit jako podezřelý v intencích Zákona č. 253/2008 Sb., tedy že by tento obchod mohl sloužit k legalizaci výnosů z trestné činnosti nebo financování terorismu, je vždy povinností obchod nahlásit**.**

Všechny pracovníky dostupné informace jsou předmětem neprodleného oznámení o zjištěném obchodu, které je podáno přímo compliance koordinátorovi, přímému nadřízenému, nebo pověřenému pracovníku oddělení AML, který rozhodne o dalším postupu. **Oznámení je třeba učinit bez zbytečného odkladu**, nejpozději však do 3 kalendářních dnů od zjištění obchodu a to pokud nehrozí nebezpečí zmaření nebo podstatného ztížení zajištění výnosů

[10] Compliance = odbor dohlížející na dodržování souladu firemních dokumentů s právními pravidly ČR

z možné trestné činnosti, v opačném případě je zapotřebí **informovat** pověřeného pracovníka **neprodleně**.

Tab. č. 4: Statistika FAÚ MF ČR 2011 - 2013

	2011	2012	2013
Počet přijatých oznámení o podezřelém obchodu	1 970	2 191	2 721
Počet podaných trestních oznámení	256	429	547
Počet podaných trestních oznámení se zajištěním finančních prostředků	96	164	177
Výše zajištěných finančních prostředků Finančním analytickým útvarem [v mil. CZK]	808,12	1 005,77	3 003,6
Počet řízení o porušení mezinárodních sankcí	8	33	23

Zdroj: http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/vysledky-cinnosti-financniho-analytickeh/2013, 2014

Při oznamování podezřelého obchodu na FAÚ MF ČR je nutné zajistit a sdělit především následující informace:

- identifikace všech subjektů, kterých se oznámení týká,
- zda (případně kdy) byl obchod proveden,
- popis předmětu oznamovaného obchodu - vždy je nutné vyjmenovat důvody, proč je oznamovaný obchod hodnocen jako podezřelý,
- všechny další informace, které s klientem nebo obchodem souvisí
- Oznámením podezřelého obchodu není dotčena povinnost oznámit skutečnosti nasvědčující spáchání trestného činu.

Oznámení o podezřelém obchodu pověřenému pracovníkovi lze následně provést:

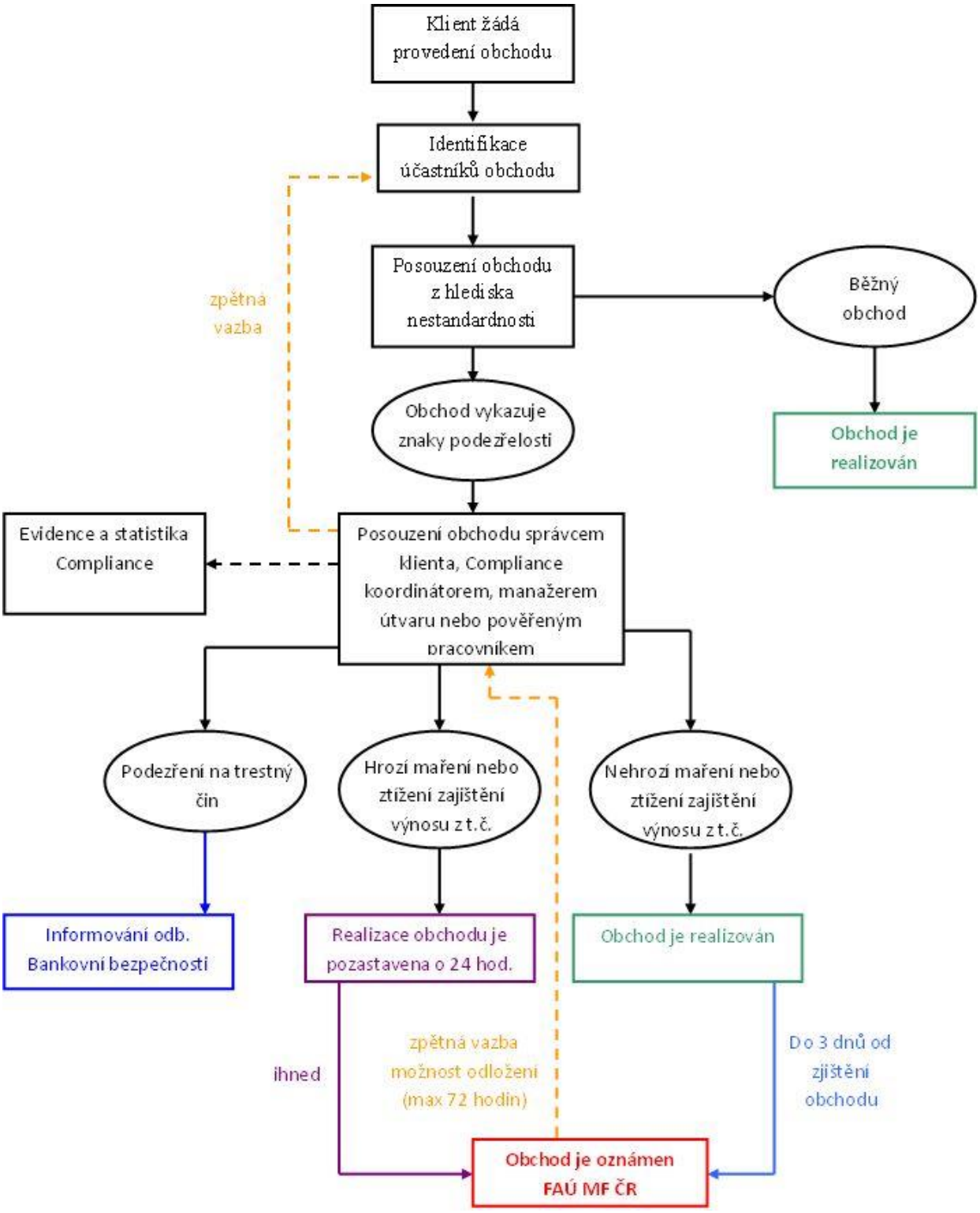
- prostřednictvím vyplněného formuláře Oznámení podezřelého obchodu (dále jen OPO),

- e-mailovou zprávou nebo v urgentních případech telefonickým sdělením,
- V případě, kdy je podezřelý obchod detekován v aplikaci SironAML (viz níže), jsou všechny získané informace soustřeďovány v oznamovací části této aplikace.

6.7 Zodpovědnost zaměstnanců

Žádný zaměstnanec banky nesmí svým jednáním umožnit obcházení mezinárodních sankcí. Takovým jednáním může být například vynechání, vymazání nebo změnění údajů na platebním příkazu, nebo strukturování transakcí s cílem zamaskovat účast sankcionované strany. Pokud má zaměstnanec podezření, že dochází k pokusu o obcházení mezinárodních sankcí, je povinen oznámit tuto skutečnost oddělení AML. [24]

Obr. č. 7: Postup vyhodnocení podezřelého obchodu



Zdroj: vlastní tvorba a [24], 2014

6.8 Možná vyhodnocení podezřelého obchodu

V zásadě existují dvě základní varianty postupu při oznámení podezřelého obchodu:

1) Podezřelý obchod – avšak nehrozí zmaření nebo podstatné ztížení zajištění výnosů z trestné činnosti.

Standardně se provede příkaz klienta (bankovní operace) a bez zbytečného odkladu odešle zpracovatel pověřenému pracovníkovi identifikaci účastníků obchodu a informace k celému případu (nejpozději do 3 kalendářních dnů) na formuláři OPO.

2) Podezřelý obchod – pokud hrozí zmaření nebo podstatné ztížení zajištění výnosů z trestné činnosti.

Zpracovatel přijme příkaz klienta a okamžitě informuje jednoho z Compliance koordinátorů, svého nadřízeného nebo pověřeného pracovníka, který rozhodne o případném odkladu splnění příkazu klienta.

6.9 Odklad splnění příkazu klienta

Lhůta 24 hodin odkladu příkazu klienta se počítá od okamžiku, kdy je OPO přijato FAÚ MF. FAÚ MF ČR může prodloužit odklad příkazu klienta o dalších 48 hodin, tzn. celkem maximálně 72 hodin.

Pokud FAÚ MF ČR nepodá **po uplynutí 72 hodin** v předmětné věci trestní oznámení, na základě kterého mohou být finanční prostředky např. zajištěny, může být na základě písemného souhlasu pověřeného pracovníka příkaz klienta proveden.

6.10 Příklad z pohledu pracovníka pobočky banky

Pokud klient vkládá v hotovosti na svůj osobní účet 1.000.000 Kč a zároveň předává bance příkaz k zahraniční platbě v e stejné částce, jejímž příjemcem bude právnický subjekt sídlící na Britských Panenských ostrovech, tzn. v OffShore[11] zóně. Dle dalších zjištění také klient pobírá dlouhodobě sociální dávky v nezaměstnanosti a jeho majetkové poměry neodpovídají výši vložené částky. Dosavadní výše transakcí jeho účtu však dosahovaly maximálně tisíců

[11] OffShore – sídlo společnosti je v zemích s nízkou nebo žádnou daňovou zátěží

Kč a v některých případech již účet vykazoval debetní zůstatek. Je nutné uplatnit následující postup.

Klienta před přijetím samotného příkazu k zahraniční platbě je třeba upozornit na možný odklad realizace transakce o 24 hodin v souvislosti se zákonem č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. A dále informovat jednoho z compliance koordinátorů, svého nadřízeného nebo pověřeného pracovníka.

6.11 Zachování mlčenlivosti zaměstnanců

Každý zaměstnanec banky je povinen zachovávat mlčenlivost o vnitřním šetření, oznámení podezřelého obchodu a úkonech činěných FAÚ MF ČR ve vztahu ke třetím osobám, včetně osob, jichž se takové informace přímo týkají. Povinnost mlčenlivosti trvá i po skončení pracovně právního či jiného smluvního vztahu k bance.

Případné porušení povinnosti mlčenlivosti je posuzováno dle zákona č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů a současně ze strany vedení banky jako zvlášť závažné porušení pracovní kázně. Zároveň je porušení mlčenlivosti podle ustanovení §38 zákona č. 253/2008 Sb. přestupkem, za který lze uložit v řízení podle zákona o přestupcích pokutu až do výše 1.000.000 Kč. Tím není dotčena odpovědnost za škodu, která tím osobě, jíž se vyzrazené údaje týkají, vznikla, ani případná trestní odpovědnost toho, kdo porušil povinnost mlčenlivosti.

6.12 Orgány vůči kterým se nelze povinnosti mlčenlivosti o oznámení podezřelého obchodu dovolávat

Tyto orgány vyjmenovává zákon č. 253/2008 Sb. a mohou jimi být např. Česká národní banka, orgány činné v trestním řízení, Národní bezpečnostní úřad, Bezpečnostní informační služba. Případné žádosti těchto orgánů vyřizuje výhradně pověřený pracovník, který může za tímto účelem požadovat spolupráci ze strany kteréhokoli zaměstnance banky.

6.13 Povinnost uchovávat údaje

Banka je povinna uchovávat identifikační údaje, jakož i údaje a doklady o obchodech spojených s povinností identifikace **po dobu nejméně 10 let** od uskutečnění obchodu. Tato

lhůta je přímo stanovena Zákonem č. 253/2008 Sb. a začíná běžet prvním dnem roku následujícího po roce, ve kterém byl proveden poslední úkon obchodu**.**

6.14 Důsledky neplnění a porušování povinností pro banku

Za porušení nebo nesplnění povinností uložených Zákonem č. 253/2008 Sb. může příslušný orgán (FAÚ MF ČR, ČNB) uložit bance **pokutu až do výše 50.000.000 Kč.** Dlouhodobé nebo opakované porušení povinnosti je důvodem k odnětí oprávnění k podnikatelské nebo jiné samostatné výdělečné činnosti podle zvláštního předpisu.

6.15 Důsledky pro konkrétní zaměstnance banky

Zatímco dříve bylo nutné pracovníkovi banky prokázat úmyslně napomáhání k legalizaci výnosů z trestné činnosti, v současné době je pracovník banky trestně postihnutelný i pokud tak učiní z pouhé nedbalosti.

6.16 Automatický monitoring pomocí aplikace SironAML

Aplikace SironAML je v UniCredit Bank Czech Republic and Slovakia, a.s. komplexním IT řešením oblasti prevence praní špinavých peněz a financování terorismu. Povinnosti požadované v rámci prevence stanové zákonem a bankovními pravidly jsou pomocí SironAML aplikovány na veškeré bezhotovostní transakce v rámci bankovních systémů. Jedná se tak o nadstavbový modul, ve kterém probíhá nejen ověření plateb ale i chování a průběžné sledování a vyhodnocování klienta během obchodního vztahu z pohledu problematiky a prevence legalizace výnosů z trestné činnosti a financování terorismu.

K vyhodnocení neobvyklého chování klientů používá banka tzv. scénáře. Za administraci a nastavení parametrů scénářů je odpovědné oddělení AML. Parametry scénářů mohou být upravovány, popřípadě mohou být přidány nové scénáře a to v návaznosti na trendy v chování klientů, podněty z FAÚ MF ČR nebo přímo z banky UniCredit**.**

Každý ze scénářů je ohodnocen určitým počtem bodů, které se v případě naplnění několika scénářů u jednoho klienta sčítají, a to vždy za jeden den scoringu[12] (nikoli za několik scoringů

[12] Scoring = bodové ohodnocení klienta

zpětně). Klient, popřípadě jeho účty nebo jeho transakce, je vyhodnocen scoringem jako podezřelý, pokud naplnil scénáře, jejichž celkové skóre přesáhlo podezřelou mez. Skutečnost, že klient byl vyhodnocen jako podezřelý aplikací SironAML, je považována za rizikový faktor dle zásady „Poznej svého klienta“.

U zahraničních platebních příkazů je banka povinna prověřit, zda se nenachází na seznamu osob spojených s uplatňováním mezinárodních sankcí. V rámci monitorování transakcí tak aplikace SironAML využívá seznam vydaný Americkým ministerstvem financí.

Konkrétně seznam vydává a aktualizuje americký Úřad pro kontrolu zahraničních aktiv (anglicky The Office of Foreign Assets Control, dále jen OFAC). Spravuje a prosazuje tak ekonomické a obchodní sankce na základě americké zahraniční politiky a národní bezpečnosti. Tento úřad má za cíl prosazování sankcí vůči cizím zemím a režimům, teroristickým organizacím, mezinárodním drogovým překupníkům, kteří se podílejí na činnosti spojené s šířením zbraní hromadného ničení, a dalších hrozeb pro národní bezpečnost, zahraniční politiku nebo ekonomiku Spojených států. Seznam OFAC je vydáván americkým úřadem, avšak mnohé z těchto sankcí jsou zařazeny z rozhodnutí Organizace spojených národů a dalších mezinárodních mandátů, jsou tedy multilaterálního rozsahu, a zahrnují úzkou spolupráci se všemi spojeneckými vládami. [11] Tyto sankce jsou tak platné i pro členské země Evropské unie a banka UniCredit je taktéž aplikuje ve své AML politice.

Další mezinárodně uplatňované sankce, které jsou v České republice právně závazné a jsou v souladu se **zákonem č. 69/2006 Sb. o provádění mezinárodních sankcí** jsou:

- **Dle nařízení Rady EU** - Treaty on the Functioning of the European Union - **TFEU** (aktuálně např.: Nařízení Rady EU č. 269/2014 - sankce přijaté v souvislosti s událostmi na Ukrajině.
- **Dle rezoluce Rady bezpečnosti OSN** - Compendium of United Nations Security Council Sanctions Lists.

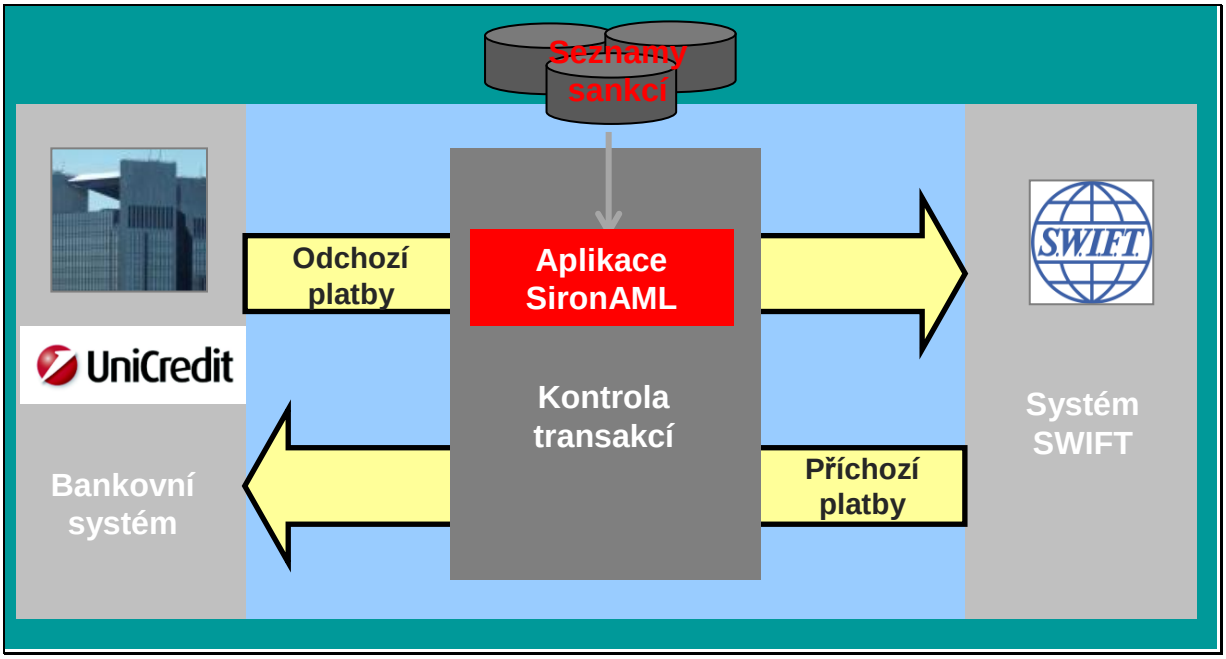
Pokud je aplikací SironAML nalezeno podezření na shodu mezi údaji o plátci nebo příjemci s údaji v sankčních seznamech, je taková platba automaticky zadržena systémem. Následně je přesunuta do zvláštní složky, která je pracovníky periodicky kontrolována. Dále provede zaměstnanec šetření celého obsahu zprávy a postupuje dle výsledku následujícím způsobem:

- v případě, že podezření není potvrzeno, platbu potvrdí a propustí k dalšímu zpracování,

- v případě, že je podezření potvrzeno, neprodleně e-mailem postoupí všechny dostupné informace o platbě, včetně důvodu zadržení (údaje o shodě) na oddělení AML banky na adresy kontaktních osob,
- zaměstnanci oddělení AML věc posoudí a rozhodnou o dalším postupu.

V případě, že dojde z rozhodnutí oddělení AML ke zrušení platby a vrácení prostředků plátci, informuje banka UniCredit příslušného klienta automatickým vygenerováním e-mailu s informací o zrušení platby.

Obr. č. 8: Schéma kontroly transakcí



Zdroj: [24]

6.17 Levenshteinův algoritmus dohledání shody

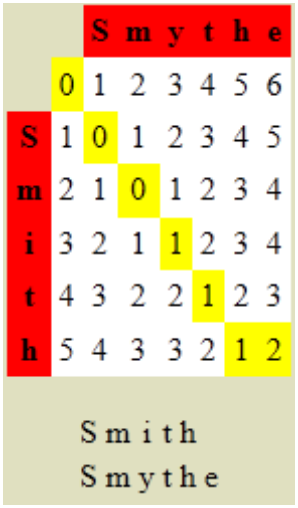
Vyhledávání v seznamech sankcí probíhá jak podle dokonalé shody, tak principem vyhledávání podřetězců. Tento systém má aplikovaný takzvaný Levenshteinův algoritmus pro výpočet minimální editační vzdálenosti. Celý proces dohledávání shody tedy funguje na principu dynamického programování. K určení zda je daný řetězec shodný s tím v sankčním seznamu dochází po virtuálním sestavení tabulky se stejným počtem řádků jako má hledaný řetězec písmen a počtu sloupců odpovídající délce prohledávaného textu. [9] Celý

proces dohledávání shody je tedy velmi sofistikovaný a nejde jen o shodu textu jako takového, ale i o všechny jeho možné varianty. Princip použitého algoritmu je vyjádřen níže.

Příklad: testování shody řetězce Smith a Smythe:

Levesthainova editační vzdálenost je zde rovna 2. Dle nastaveného algoritmu následně program vyhodnotí, zda je shoda dostatečná pro zadržení transakce či nikoliv.

Obr. č. 9: Sestavení tabulky Levenshteinova algoritmu



Zdroj: http://odur.let.rug.nl/~kleiweg/lev/, 2014

7 Zneužití platebních karet

Zneužití platebních karet patří neodmyslitelně k základním praktikám **nezákonného obohacení**. Aby bylo možné sledovat a posuzovat transakce a autorizace, je nutné nejprve získat potřebná data. V bance UniCredit jsou vydávány karty společností **Visa a MasterCard**. Pro správu a komunikaci s karovými společnostmi jsou využívány softwarové aplikace MASTERCARD.NET a VISAONLINE.

Nadstavbou těmto systémům je autorizační systém kartového centra **ONLINE**. Ten obsahuje databáze typu Microsoft Access, které obsahují transakční a autorizační data. Pro monitoring transakcí jde o Access databázi Transaction Monitoring a pro monitoring autorizací se používá databáze nazývaná Monitoring Autorizací. Každý den probíhá podrobné monitorování transakcí a autorizací ve všech relevantních IT systémech. Z tohoto monitorování je následně večer při uzavírání účetního dne vygenerován jednorázový soubor, který se následně nahrává do systému ONLINE a ten tak stále udržuje ve svých databázích aktuální data.

Další aplikací přímo zaměřenou na odhalování podvodů je **FraudGuard**. Tento systém je přímo dodáván od emitentů platebních karet. Jedná se o takzvaný issuer[13] monitoring. Tento systém poskytuje mimo monitorovací funkci i mnoho dalších užitečných modulů, které slouží k prevenci, odhalování a následnému šetření podvodného jednání na úseku platebních karet. Systém FraudGuard je spravován bankou, avšak jeho vývoj a provoz spadá přímo pod emitenty platebních karet.

7.1 Oddělení Fraud&Security

Pro účely fraud managementu platebních karet je v UniCredit bance zřízeno oddělení **Fraud&Security**. Jeho činnosti se týkají zejména monitorování transakcí a autorizací jak držitelů karet na straně jedné (tzv. Issuerská část), tak obchodníků akceptujících přijímání platebních karet (tzv. Acquirerská[14] část). Toto oddělení obsluhuje a vyhodnocuje data z aplikací ONLINE a FraudGuard.

Hlavní činnosti oddělení Fraud&Security jsou:

1. Issuer monitoring

[13] Issuer - emitent
[14] Acquirer - nabyvatel

- Case Management
- ONLINE monitoring

2. Acquirer monitoring
    - Monitoring autorizací
    - Monitoring transakcí
3. Spolupráce s policií České republiky
4. Spolupráce s oddělením compliance
5. Reporty společnostem VISA a MASTER CARD
6. Statistiky
7. Schvalování smluv
8. Evidence zadržených karet (v bankomatech nebo u obchodníků)
9. Schvalování odměn obchodníkům
10. Školení obchodníků
11. Rozhodování o zadávání účetních dokladů – autorizace

7.2 Monitoring obchodníků

Systém monitoringu obchodníků v bance UniCredit shromažďuje data ve dvou databázích aplikace Microsoft Access v systému ONLINE s tříměsíční historií. Pravidelně jsou generované reporty, vytvořené na základě výběru dat podle předem nastavených kritérií. Získané informace se analyzují a v případě podezření na podvodnou transakci je zahájeno šetření. Kontaktují se obchodníci a emitent, nebo se ověřují podezřelá čísla karet a transakcí s dalšími kompetentními autorizačními centry v České republice. **V případě potvrzení podvodné transakce** podává oddělení Fraud&Security **trestní oznámení České policii**. Systém monitoringu významným způsobem snižuje operační riziko v oblasti zneužití platebních karet, ať již preventivním způsobem či svým včasným zásahem dokáže eliminovat výši způsobených škod.

7.3 Kontrola rizikovosti obchodních partnerů

Produktový specialista UniCredit předá oddělení Fraud&Security následující podklady: dotazník partnera, identifikaci, evidenční kartu klienta spolu s kopií průkazu totožnosti oprávněného obchodního partnera, hodnocení provozovny a doplňující dokument. Po obdržení smluvní dokumentace provede oddělení Fraud&Security kontrolu, zda je dokumentace kompletní. Dle konkrétní situace může požadovat doplnění podkladů, jako například o výpis z firemního nebo privátního účtu, daňové přiznání za poslední aktuální období atd. Také může být dožádána obchodní inspekce (pokud nebyla již provedena a není součástí předaných podkladů). Oddělení Fraud&Security prověří vlastní negativní databáze a reference ostatních partnerů. Pověřený pracovník pak zkontroluje v interní databázi vypovězených obchodníků, jestli zde nemá firma uvedená v dotazníku záznam. Následuje kontrola v databázích asociací. Databáze vypovězených obchodníků je průběžně aktualizována a obchodníci jsou do ní doplňovány z e-mailových zpráv, ve kterých ostatní banky oznamují vypovězení obchodního partnera. I oddělení Fraud&Security banky UniCredit má povinnost v případě vypovězení obchodníka informovat ostatní acquirerské banky. [24]

7.4 Reporty monitoringu transakcí

Aplikace ONLINE umožňuje tvorbu reportů, které oddělení Fraud&Security využívá pro svoji investigativní činnost. Tyto reporty slouží nejenom k **vyšetřování** ale i při **řešení případných reklamací**, kdy tato databáze poskytuje rychlé a obsáhlé informace o transakcích. Reporty tak využívají i ostatní oddělení banky jako například finanční nebo účetní. Pro lepší představu o reportovací činnosti je níže uveden popis výběru ze seznamu reportů:

1. **Multiple-card-usage:** report obsahuje seznam všech čísel karet, které překročily limit počtu a částky transakcí, procesované pod jedním číslem karty.
2. **Average-manual-key-entry-transaction–amount:** report obsahuje seznam provozoven obchodníků, ve kterých byla překročena průměrná denní částka manuálně typovaných transakcí.
3. **Average-manual-key-entry-transaction–numer:** report obsahuje seznam provozoven obchodníků, ve kterých byl překročen denní průměr počtu manuálně zadávaných transakcí.

4. **New-merchant-monitoring:** report obsahuje přehled všech zpracovaných transakcí nových provozoven za sledovaný den, které byly při schvalování smluv vytipovány jako potenciálně problematické. Nové provozovny jsou monitorovány po dobu tří měsíců.
5. **Facultative-deposit-aktivity:** report obsahuje seznam obchodníků, v jejichž provozovnách proběhla platba platební kartou po tříměsíčním období bez platby kartou.

7.5 Zadržené platební karty

Zadržené platební karty mohou přicházet z několika zdrojů, jsou to karty zadržené u smluvních obchodních partnerů UniCredit banky, karty zadržené v bankomatech UniCredit, karty nalezené a odevzdané na pobočkách banky a karty zadržené v bankomatech společnosti EURONET, pro kterou je UniCredit smluvním partnerem na provozování sítě bankomatů. Při doručení jakékoli zadržené platební karty, provádí oddělení Fraud&Security **kontrolu bezpečnostních prvků** platební karty a historie autorizací v síti obchodních partnerů.

7.6 Platební karty zadržené smluvními obchodními partnery UniCredit

U těchto způsobů zadržení platebních karet je **možnost vyplácení odměn** (ekvivalent 100 USD) za zadržení platební karty. Pro zhodnocení, zda odměnu vyplatit, je důležité nahlédnout do transakčního monitoringu a prohlédnout autorizační historii dané platební karty. Aby mohla být odměna uznána, od vydavatele platební karty musí být při autorizaci pokyn k zadržení platební karty. Posouzení probíhá individuálně a odměna není vyplácena pouze v případě, když existuje podezření, že obchodník těchto odměn zneužívá, popř. testuje nalezené karty atd. Pozorně se postupuje také v případech, kdy je platební karta zadržena při autorizacích na velmi nízké částky - např. 10 Kč. V těchto případech se může jednat o platební karty, které obchodník nalezl na své provozovně a pokouší se získat odměnu. **Odměny za zadržení platební karty se vyplácejí pouze konkrétním pracovníkům**, kteří kartu zadrželi, nikoli vedoucím směny, majitelům provozovny a podobně.

7.7 Nalezené platební karty

Za nalezené platební karty se **odměny nevyplácejí**. Provede se kontrola bezpečnostních prvků platební karty a historie v autorizačním monitoringu, do kterého je zaznamenán nález platební karty. Karty se odevzdávají bankovnímu oddělení Authorization&Processing. Pokud se jedná o platební kartu vydanou UniCredit bankou, provede se **kontrola bezpečnostních prvků** platební karty a historie autorizací a následně bude zařazena mezi platební karty určené ke **skartaci**.

7.8 Spolupráce s oddělením compliance

Na oddělení compliance banky se zasílá veškerá korespondence a zpracované dotazy Policie České Republiky. Pracovníci Fraud&Security hlásí podezřelé transakce a veškeré transakce převyšující částku 15.000 EUR. Pracovníci compliance se naopak na Fraud&Security obracejí s požadavky na zjištění detailů transakcí a jiných údajů ze systémů ONLINE, VISAONLINE, FraudGuard, atd.

7.9 Spolupráce s oddělením bankovní bezpečnosti

Odbor bankovní bezpečnosti v případě dotazu Police ČR zajišťuje záznamy z kamerových systémů poboček a bankomatů. Pracovníci oddělení Fraud&Security zasílají dboru bankovní bezpečnosti poznatky týkající se ohrožení bezpečnosti bankomatů, terminálů, podezření na **phishing**, **pharming** atd. Také se zasílají oddělení bankovní bezpečnosti formou e-mailové zprávy informace o podání trestního oznámení a jeho kopie.

7.10 Komunikace s policií České republiky

Komunikace s Policií České Republiky probíhá na základě dotazů, které Police ČR zasílá na kartové centrum banky UniCredit **prostřednictvím veřejné datové sítě do datové schránky** nebo prostřednictvím České pošty formou dopisů. Na tyto dotazy odpovídá pracovník Fraud&Security v případech, kdy se tyto dotazy týkají platebních karet a jsou, v případě dopisů, opatřeny razítkem státního zástupce, nebo souhlasem držitele platební karty s poskytnutím informací pro potřeby Policie ČR. V případě doručení do datové schránky musí být opatřeny **elektronickým podpisem** případně elektronickou značkou Pokud není dotaz

s razítkem státního zástupce a s elektronickým podpisem příp. značkou, nebo se souhlasem držitele platební karty, vyžádá si pracovník doplnění u Policie České republiky.

7.11 Trestní oznámení

Trestní oznámení je podáváno v případech, kdy je zneužita platební karta vydaná UniCredit bankou a držitel platební karty není schopen z nějakého důvodu podat trestní oznámení sám. K trestnímu oznámení vyhotoví pracovník Fraud&Security přehled autorizací provedných danou platební kartou a zašle ho na Policejní oddělení sídlící v místě, kde vznikla největší škoda. Následně trestní oznámení odešle pracovník i s přílohou vedoucímu oddělení bankovní bezpečnosti.

7.12 Vnitřní kontrolní systém

Vnitřní kontrolní systém je obecně popsán ve schváleném vnitřním předpisu banky. **Každý pracovník kartového oddělení má přiděleno osobní personální číslo**, pod kterým se přihlašuje do všech systémů. Každý používaný systém navíc **vyžaduje vložení hesla**, které si každý pracovník zvolí samostatně. Po vypršení platnosti hesla si systém vyžádá vložení a potvrzení nového hesla.. Oprávnění pro přístup do jednotlivých systémů podléhá schválení nadřízeného a následnému schvalovacímu procesu.

Další oprávnění jednotlivých pracovníků je řízeno udělováním plných mocí a udělováním zvláštních plných mocí tak, aby pracovník mohl provádět požadované úkony při své pracovní činnosti pro banku. Pravidelné testování kontrolního systému probíhá samostatně, nebo na vyžádání ve spolupráci s příslušnými útvary banky. Korespondence, která se zasílá mimo banku **musí být vždy podepsána nejméně dvěma pracovníky**.

7.13 Další kontrolní mechanismy oddělení Fraud&Security:

Na oddělení je aplikován **průběžný monitoring** a kontrola činnosti oddělení Fraud&Security příslušným vedoucím. Zjištěné nedostatky jsou **ihned** řešeny, případně projednány s přímým nadřízeným a přijatá opatření zanesena do pracovního manuálu, případně pracovní knihy při nejbližší aktualizaci. **Mimořádné události jsou neprodleně hlášeny** vedoucímu kartového oddělení a vedoucímu operačního rizika UniCredit. Vše je dokumentováno. **Průběžně jsou zároveň sledována a vyhodnocována potenciální rizika** s ohledem na jejich závažnost,

a případně jsou přijímána opatření ke snížení takových rizik změnou nastavených parametrů v monitorovacích systémech. Pokud se prokáže podvod a je potřeba vyhotovit škodní protokol, poté se případ předá oddělení bankovní bezpečnosti. To následně zajistí zápis škodního případu do archivní evidence.

8 Zhodnocení úrovně řízení operačních rizik banky UniCredit

Tak jako každá banka i UniCredit se snaží řízení rizik neustále zdokonalovat a rozvíjet. Momentální úroveň zabezpečení elektronických kanálů, bankomatů, pobočkových pokladen i celý proces kontroly proti praní špinavých peněz je na velmi vysoké úrovni. Banka nabízí jak standardní zabezpečení, tak i řadu příplatkových. Například u elektronických kanálů je to možnost tokenu nebo vzdáleného podpisu. Řadí se také mezi technologické inovátory s aplikací Smart klíč, která je velmi moderní a dle nejnovějších trendů mobilní autentizace.

Na druhou stranu se však nevrhá bezhlavě do všech možných novinek v oblasti bezhotovostního placení. Pokud není daná technologie dostatečně vyzkoušená a zabezpečená, postupují specialisté UniCredit velmi rozvážně. To je i případ trendu poslední doby, kdy přišlo do módy bezkontaktní placení platební kartou. Jde o rychlý způsob úhrady pomocí speciálních terminálů a k nim přizpůsobených karet, kdy k platbě není nutná autorizace a karta ani není do terminálu vkládána. Při těchto platbách nedochází k zadání PINu ani podpisu a vše se odehrává v podstatě anonymně. Veškeré zabezpečení je jen otázkou nastaveného limitu, který bývá zpravidla kolem 500 Kč na jednu transakci. Přestože se jedná o klienty vyhledávanou technologii, není zatím rozhodnuto o jejím nasazení v rámci banky UniCredit. V těchto případech je postup banky spíše konzervativní, avšak to je dáno nastolenou úrovní její bezpečnostní politiky. Ztráta reputace bývá někdy větší přítěží a újmou, než zdánlivé nepohodlí stávající klientely.

Velká důležitost je věnována školení zaměstnanců a jejich informovanosti. Pravidelně jsou pořádány konference a semináře na téma bezpečnosti a formou e-learningu[15] jsou všichni nuceni aktivně se danou problematiku naučit. Každoročně jsou tyto elektronické kurzy obnovovány a aktualizovány. Systémově jsou tak lidé v UniCredit vedeni k prohlubování svých znalostí v oblasti fraud managementu a interaktivně musí umět vyřešit několik přednastavených podvodných scénářů. Tento proces školení je velice efektivní a přebírají ho i některé další finanční ústavy.

V rámci evropských i celosvětových měřítek jsou bankovní procesy proti podvodům nastaveny správně a v požadované shodě s legislativou. V komparaci s ostatními českými bankovními ústavy nelze vytknout konkrétních slabin. Avšak bylo by mylné, přestat

[15] e-learning – elektronická forma výukových kurzů

na dalším rozvoji pracovat. V oblasti podvodných jednání není proces ochrany nikdy v konečném bodě.

Správně bylo investováno nemalé úsilí a finanční prostředky do nasazení programu SironAML, který účinně filtruje podezřelé transakce. Ten představuje momentálně nejvyšší úroveň automatického screeningu[16] a řadí se tak ke světové špičce. Do budoucna se tento software rozšíří i do dalších oblastí fraud managementu a zahrne do své činnosti i správu procesů KnowYourCustomer. Zautomatizování celého procesu je funkcí dalšího modulu aplikace SironAML, který banka plánuje nasadit a využívat.

V oblasti bankomatů vlastní banka jednu z nejmodernějších sítí těchto strojů. Všechny jsou již vybaveny antiskimmovacími nástavci a úpravami. Pro znesnadnění podvodů je také většina umístěna uvnitř budov a není možné k nim přistupovat přímo z ulice. Je tak snadnější i sledování jejich okolí pomocí kamerových systémů. Takové zabezpečení je momentálně maximální možné a tomu odpovídá i nízký počet pokusů o napadení v porovnání s bankomaty ostatních společností.

Není jednoduché všechny zabezpečení udržovat stále na té nejvyšší úrovni. Je však nezbytné průběžně hledat možná zlepšení. V tomto ohledu je asi největší slabinou riziko vnitřních podvodných jednání. Ochrana proti nim je důležitá a v mnoha případech trochu opomíjená. Je nezbytné **postupovat pečlivě a systematicky** a dodržovat nastolený sofistikovaný **systém vnitřních kontrol**, postupů a procesů. Nedílnou součástí je i pravidelný vnitřní bezpečnostní audit. Vzhledem k jeho finanční a časové náročnosti však dochází často k odložení jeho konání. Iniciativa musí v tomto případě přijít od nevyššího vedení, které dohlíží na řádné konání těchto kontrol.

Jako většina ostatních bankovních procesů je i úroveň řízení operačních rizik přímo závislá na odbornosti zaměstnanců. Se vznikem nových bankovních domů dochází často k přetahování odborníků. Tomuto se nevyhne ani UniCredit a musí tak do budoucna plánovat jak si své klíčové zaměstnance udržet. Aby byla kontinuita a kvalita procesů zachována, bude nutné nejen **udržet stávající**, ale i vychovávat nové talentované **zaměstnance**. Ačkoliv banka nabízí absolventům škol **trainee programy**[17], bylo by vhodné prohlubovat v tomto směru přímou spolupráci s univerzitami a zajistit tak do budoucna příliv nových kvalifikovaných sil.

[16] Screening – vyšetření, prošetření

[17] Trainee program - speciální rozvojový program určený čerstvým absolventům vysokých škol

Banka UniCredit je rozvětvenou společností s vysokým počtem zaměstnanců i klientů. Pouze správně nastavené a řízené procesy fraud managementu mohou všechny ochránit před podvodnými pokusy a pokud už k nim dojde, k minimalizaci ztrát. Finančně i organizačně je řízení operačních rizik velmi náročný a nikdy nekončící proces, avšak nezbytný pro dlouhodobé úspěšné fungování banky.

Závěr

Závěrem mé práce bych chtěl vyzdvihnout trend v oblasti podvodů ve finanční sféře: „tak, jak se vyvíjejí nové technologie, vyvíjejí se i způsoby podvodných jednání.“ Velké úsilí v oblasti fraud managementu se tedy primárně zaměřuje na prevenci a předcházení podvodných jednání. Všechna rizika však nikdy definovat nelze a útočníci bývají vždy o jeden krok napřed. Účinné řízení operačních rizik je velmi nákladné a zdálo by se, že pro organizaci mnohdy nevýhodné. Avšak útočníci nejsou pro banku hrozbou jen finanční, ale ohrožují svými útoky i její reputaci. Tak jak musí firma investovat do své reklamy a propagace, musí účinně investovat i do své obrany. Nedílnou součástí je i obrana vlastních zákazníků.

V úvodu práce jsou vytýčeny analyzované cíle, které jsem se dále snažil rozvinout a popsat. První část definuje typy podvodů a oblasti kde k nim může ve finančních institucích docházet. Následuje popis hotovostního a bezhotovostního platebního styku. Dále jsou upřesněny pojmy jako domácí platební styk a podvodné jednání nazývané phishing. S tím souvisí i oblast zahraničního platebního styku. Je objasněna jeho forma a nové způsoby plateb SEPA a Europlatba. Další část je zaměřena na oblast podvodů na poli platebních karet, se kterými se každý z nás dennodenně setkává. Vysoce aktuální je způsob podvodu nazývaný skimming. V práci je uvedeno i jak se proti němu účinně bránit. Jako další možný typ podvodu je vybrána Lisabonská smyčka, která názorně ukazuje jednoduchost, se kterou jsou podvodníci schopni klienta připravit o jeho hotovost. Nejnovější trend v kopírování platebních karet ilustruje technika zvaná shimmimg. Ve výčtu nesmí chybět ani shoulder surfing, který je jednoduchý, ale přesto stále účinný. Na závěr první části jsou uvedeny zákony, normy a vyhlášky související legislativy České republiky, které podvodné jednání definují, nebo se k němu vztahují.

V praktické části je představena banka UniCredit. Následuje výčet jejích základních činností a dále druhy kanálů pro komunikaci s klienty v rámci bezhotovostního platebního styku. Důležité jsou také typy zabezpečení elektronické komunikace, které banka využívá a nabízí. V práci jsou analyzována jednotlivá opatření, která banka v prevenci a boji s podvodnými jednáními, dělá. Jsou definovány oblasti důležité pro rozvoj fraud managementu jako např.: hodnocení rizik, lidské zdroje, výzkum a vývoj a informační technologie.

První důležitou oblastí k hlubší analýze je zvolena obrana proti praní špinavých peněz a financování terorismu. Je uvedena politika, kterou v této oblasti banka uplatňuje, jednotlivé

procesy praní špinavých peněz a historický vznik této podvodné techniky. Podrobněji je popsán postup jak se zachovat v případě podezřelých obchodů. Jednotlivé kroky, které by měli všichni zaměstnanci znát vycházející ze základní klasifikace klientů a následném postupu v případě, že se o podezřelý obchod opravdu jedná. Kam obchod hlásit, jaké orgány státní moci mají tuto oblast podvodů v kompetenci a co hrozí zaměstnancům a bance v případě neplnění těchto povinností? I na tyto otázky dává praktická část odpovědi.

Další oblastí podrobené analýze řízení rizika je zneužití platebních karet. V práci je uvedeno který odbor banky se primárně kartovými fraudy zabývá. Následují důležité činnosti a postupy k předcházení, monitorování a odhalování podvodů s kartami. Nejedná se zde pouze o klienty a jejich útočníky, ale překvapivě je třeba zvýšená opatrnost i ve spolupráci s obchodníky, kteří karty přijímají. Je popsána i součinnost s dalšími bankovními odděleními, jako jsou compliance a bankovní bezpečnost a také s policií České republiky. Nedílnou součástí je i vnitřní kontrolní systém a další kontrolní mechanizmy.

Zhodnocení úrovně zabezpečení banky, identifikace slabých míst a možný prostor pro zlepšení jsou obsahem závěrečné kapitoly.

Z dnešního pohledu je téma fraud managementu velice aktuální. Já sám se s ním setkávám ve svém zaměstnání prakticky denně. Podvody jako takové již dávno nejsou výsadou pouze jednotlivců či organizovaných skupin, nyní se o ně pokoušejí i celé státní aparáty. Z hlediska banky je tak nutné vybudovat opravdu kvalitní obrannou strategii, která zamezí a případně maximálně omezí většinu podvodného jednání. Tato iniciativa musí směrovat jak na útočníky z venčí, tak na zaměstnance a v mnoha případech i na vrcholný management. Jedná se tedy o nikdy nekončící boj a současně o boj s velkou přesilou.

Seznam tabulek

Seznam obrázků

Seznam použitých zkratek

ACFE	Americká Asociace certifikovaných vyšetřovatelů podvodů
AML	(Anti-Money Laundering) - oddělení proti praní špinavých peněz
APWG	(Anti-Phishing Working Group) - Světová asociace proti phishingu
BIC	(Bank Identifier Code) – mezinárodní bankovní kód, 8mi nebo 11ti místný alfanumerický kód jednoznačně identifikující banku nebo její pobočku
CERTIS	(Czech Express Real Time Interbank Gross Settlement) - systém mezibankovního platebního styku v České republice
ČNB	Česká národní banka
FAÚ MF ČR	Finanční analytický útvar Ministerstva financí ČR
IBAN	(International Bank Account Number) – mezinárodní jednoznačný identifikátor bankovních účtů v příslušné finanční instituci v dané zemi, vyvinutý pro zjednodušení zahraničního platebního styku.
KYC	(KnowYourCustomer) - princip poznej svého klienta
OFAC	(The Office of Foreign Assets Control) - americký Úřad pro kontrolu zahraničních aktiv
OPO	Oznámené podezřelé obchody
PIN	Bezpečnostní numerický kód
PPK	Ppolitika přijatelnosti klienta
SEPA	(Single Euro Payments Area) – jednotná oblast pro platby v měně Euro
STEP2	Evropský platební systém umožňující zpracování přeshraničních plateb do výše 50.000 EUR
SWIFT	(Society for Worldwide Interbank Financial Telecommunication) – Společnost pro celosvětovou mezibankovní finanční telekomunikaci.

Seznam použité literatury

Tištěné zdroje:

[1] ČÍRTKOVÁ, Ludmila a kol. *Podvody, zpronevěry, machinace: (možnosti prevence, odhalování a ochrany před podvodným jednáním)*. Vyd. 1. Praha: Armex, 2005, 247 s. ISBN 80-86795-12-8

[2] JAMES, Lance. *Phishing bez záhad*. 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

[3] NIGRINI, Mark J. *Forensic analytics: methods and techniques for forensic accounting investigations*. Hoboken, N.J.: Wiley, 2011, 463 s. ISBN 978-047-0890-462.

[4] ROBINSON, Jeffrey. *Pánové z prádelny špinavých peněz*. 1.vyd. Praha: Columbus, 1995, 289 s. ISBN 80-859-2806-X.

[5] SILVERSTONE, Howard a Michael SHEETZ. *Forensic accounting and fraud investigation for non-experts*. 2nd ed. Hoboken, N.J.: Wiley, 2007, 294 s. ISBN 978-047-1784-876.

Elektronické zdroje

[6] BLAŽKOVÁ, Lenka. *Fraud management aneb Předcházení podvodům ve finančních institucích.* [online]. 2012 [cit. 2014-03-10]. Dostupné z: http://www.systemonline.cz/business-intelligence/fraud-management-1.htm

[7] *Bezhotovostní platební styk*. Wikipedie [online]. [cit. 2014-03-14]. Dostupné z: http://cs.wikipedia.org/wiki/Bezhotovostn%C3%AD_platebn%C3%AD_styk

[8] *Cílem bankovních reforem je omezit spekulace a rizikové obchody*. [online]. [cit. 2014-04-12]. Dostupné z: http://ec.europa.eu/news/economy/140131_cs.htm

[9] *Levenshteinova vzdálenost*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.algoritmy.net/article/1699/Levenshteinova-vzdalenost

[10] KLUFA, František, Petr SCHOLZ a Michaela KOZLOVÁ. *Podvody v oblasti bezhotovostních plateb v ČR* [PDF]. Sdružení českých spotřebitelů, 2009 [cit. 2014-04-10]. Dostupné z: http://prevencepodvodu.cz/users/files/projekt-o-podvodech/A5_bezhotovostni_podvody.pdf

[11] *Office of Foreign Assets Control (OFAC).* [online]. [cit. 2014-04-14]. Dostupné z: http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

[12] *Odbor 24 - Finanční analytický*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.mfcr.cz/cs/o-ministerstvu/zakladni-informace/organizacni-struktura/dane-a-cla-sekce-05/odbor-24-financni-analyticky

[13] *Oversight – dozor nad platebními systémy a dalšími nástroji platebního styku*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.cnb.cz/cs/platebni_styk/oversight/#3

[14] *Popis systému CERTIS*. [online]. [cit. 2014-04-14]. Dostupné z: https://www.cnb.cz/cs/platebni_styk/certis/certis_popis.html

[15] *SEPA - Single Euro Payments Area*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.ecb.europa.eu/paym/sepa/html/index.en.html

[16] *Shimming*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.redferret.net/?p=22227

[17] *Shoulder surfing*. [online]. [cit. 2014-04-14]. Dostupné z: http://safeinternetbanking.be/en/fraud-techniques/shoulder-surfing

[18] *SKIMMING*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.policie.cz/clanek/skimming.aspx

[19] *Trestní zákoník (Česko, 2009)*. Wikipedie [online]. [cit. 2014-04-14]. Dostupné z: http://cs.wikipedia.org/wiki/Trestn%C3%AD_z%C3%A1kon%C3%ADk_(%C4%8Cesko,_2009)

[20] *Údaje o bance k 30. 9. 2013*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.unicreditbank.cz/files/download/o-bance/pdf/UCB_INFO_POVINNE_UDAJE_03_2013.pdf

[21] *Unicreditbank*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.unicreditbank.cz/

[22] *UniCredit Bank Czech Republic and Slovakia, a.s*. [online]. [cit. 2014-04-14]. Dostupné z: http://www.unicreditbank.cz/web/o-bance

[23] *Zákon o „praní špinavých peněz“, ale nejen o něm*. [online]. 2010 [cit. 2014-04-14]. Dostupné z: http://www.pojistenec.cz/zakon_o_prani_spinavych_penez.htm

Ostatní zdroje:

[24] Interní zdroje bankovní instituce

Abstrakt

ČIHÁK, Jan. *Analýza metod a nástrojů fraud managementu ve vybraném podniku*. Bakalářská práce. Plzeň: Fakulta ekonomická ZČU v Plzni, 71 s., 2014

Klíčová slova: podvod, podezřelý obchod, riziko, praní špinavých peněz, financování terorismu

Tato bakalářská práce se zabývá definováním metod a nástrojů fraud managementu a jeho analýzou ve zvolené bankovní společnosti. V teoretické části jsou podrobně vysvětleny oblasti podvodných jednání ve finanční sféře. Jsou popsány vybrané metody bezhotovostního platebního styku a jejich principy. Také jsou uvedeny obecné druhy podvodných technik. V praktické části je práce zaměřena na analýzu řízení rizik ve vybrané bance. Definování metod fraud managementu je zaměřeno na oblast praní špinavých peněz a financování terorismu a také podvodů v oblasti platebních karet. Dále jsou v práci zpracovány způsoby prevence a ochrany proti možným podvodným jednáním a popsány interakce jednotlivých bankovních odborů a oddělení, které jsou v dané problematice kompetentní.

Abstract

ČIHÁK, Jan. *Analysis of methods and tools of fraud management in a selected company*. The bachelor thesis. Pilsen: Faculty of Economics, University of West Bohemia, 71 pgs., 2014

Key words: fraud, suspicious transaction, the risk of money laundering, terrorist financing

This bachelor thesis deals with the definition of methods and tools of fraud management and analysis of selected banking company. In the theoretical part are explained in detail areas of the fraud in the financial sector. The selected methods for cashless payment transactions and their principles are described. Also the general types of phishing techniques are listed. The practical part of the thesis focuses on the analysis of risk management in the selected bank. Defining of methods of fraud management is focused on money laundering and terrorist financing and frauds targeting on credit cards. Furthermore, the work processes ways to prevent and protect against possible fraudulent behavior and describes the interaction of bank departments and units that are competent in the matter.