ZÁPADOČESKÁ UNIVERZITA

V PLZNI

FAKULTA PRÁVNICKÁ

Katedra správního práva

DIPLOMOVÁ PRÁCE

Elektronické bankovnictví

Blažim 2012 **Jiří FILÍPEK**

ZÁPADOČESKÁ UNIVERZITA

V PLZNI

FAKULTA PRÁVNICKÁ

Katedra správního práva

Oddělení finančního práva

Studijní program: magisterský

Obor: Právo a právní věda

Diplomová práce

Elektronické bankovnictví

Jméno diplomanta: Jiří Filípek

Vedoucí diplomové práce: JUDr. Petra Jánošíková, Ph.D.

Blažim 2012

Prohlášení

Prohlašuji, že diplomovou práci na téma „Elektronické bankovnictví“ jsem vypracoval samostatně a že jsem uvedl veškeré prameny, použitou literaturu a podkladové materiály, ze kterých jsem čerpal v seznamu literatury.

Blažim, březen 2012 Podpis:_____

Poděkování

Rád bych poděkoval vedoucí mé diplomové práce JUDr. Petře Jánošíkové, Ph.D. za ochotu vést individuální téma a vstřícnost, kterou mi v průběhu psaní této práce poskytovala. Můj dík v neposlední řadě patří rodině a přítelkyni za jejich trpělivost a podporu.

Jiří Filípek

Předmluva

Důvodem zvolení tématu „Elektronické bankovnictví“ byl zejména fakt, že bankovnictví, ať už chceme nebo nechceme, je nedílnou součástí našeho života. A pojem „elektronické“ vyjadřuje jakýsi technologický pokrok, který toto téma dělá o něco více zajímavějším. Hlavními použitými metodami jsou zejména analýza elektronického bankovnictví jako celku a jeho následný popis. Hlavní přínos práce spatřuji zejména ve sjednocení daných druhů e bankingu, ve vymezení možností a doporučených opatření, potřebných k minimalizaci bankovních podvodů..

Tato diplomová práce poskytuje komplexní přehled v oblasti elektronického bankovnictví. Zabývá se nejen vymezením všech druhů elektronického bankovnictví, ale také o systémech obdobných. Vymezuje českou právní úpravu dané problematiky s odkazem na právo EU. A v neposlední řadě se zabývá možnými bankovními podvody, především podvody zneužitím platebních karet či internetového bankovnictví a řešením tohoto problému.

Blažim, březen 2012 Podpis:_____

Obsah

POUŽITÉ ZKRATKY:

ČR - Česká republika

ČSR - Československá republika

EU - Evropská unie

EUR - Měna eurozóny

SWIFT - Society for Worldwide Interbank Financial Telecommunication

ČNB - Česká národní banka

BOA - Bank of America

USD - Americký dollar

USA - Spojené státy americké

PIN - Personal identity number

PUK - Personal Unlocking Key

WIFI - Wireless Ethernet Compatibility Aliance

EDGE - Enhanced Data rates for GSM Evolution

3G - Třetí generace mobilních telefonů

GSM - Globální Systém pro Mobilní komunikaci

IT - Umělá inteligence

IVR - Interaktivní hlasová odezva

OTP - One time pasword

GB - Gygabyte

WAP - Wireless aplicattion protocol

CD - Compact disc

USB - Universal Serial Bus

TAN - Tabulka autorizačních čísel

ID - Identifikace

BIC - The bank identifier code

TrZ - Trestní zákoník

DNS - Domain name system

SSL - Secure sockets layer

PDA - Personal digital assistant

MDA - Mobile digital assistant

ZPS - Zákon o platebním styku

PS - Poslanecká sněmovna

FA - Finanční arbitr

1 Úvod

Celý svět se nezastavitelně vyvíjí, technologický pokrok, který ovlivňuje snad všechny odvětví, je každým dnem výš a výš, výjimku netvoří ani bankovnictví, pro které se hlavně po roce 1990 otevřely nové možnosti. Výrazný boom prožily především informační a komunikační technologie, které mají pochopitelně největší zásluhu na dnešní podobě elektronického neboli přímého bankovnictví[1]. Velký vliv na vývoj e-bankingu má bezpochyby internet, který bankovní sféru ovlivnil, více než ostatní.

Mezi další hnací síly, které transformovaly bankovnictví, jaké známe dnes, patří změny v ekonomickém prostředí, inovace ve finančních produktech, liberalizace finančního trhu a hlavně lidská poptávka po pohodlnosti.

Hlavní rozdíl mezi elektronickým a klasickým bankovnictvím je v komunikaci mezi bankou a klientem. Klient nemusí osobně navštívit bankovní dům k vyřešení běžných bankovních úkonů nebo transakcí.

Nejvíce výstižný název pro e-banking je zřejmě „vzdálené bankovnictví“, a to proto, že klient může být se svými peněžními prostředky v kontaktu 24 hodin denně, 356 dní v roce[2], tedy bez fyzické návštěvy banky.

Tato technologie má řadu výhod, jak pro banku, tak pro klienta, a to jak v úspoře času, který je v dnešní době stále důležitější, tak i v poskytování pohodlí při provádění bankovních operací. Na druhou stranu klient potřebuje technické zázemí, bez kterého je elektronické bankovnictví nemožné. Výhoda pro banku spočívá v šetření pracovních pozic, tudíž si může dovolit zlevnit elektronické operace, které protistrany ocení. Ovšem každá mince má dvě strany a e-banking není výjimkou. Mezi největší negativa tohoto fenoménu patří přenos osobních a důvěrných dat o klientovi, jeho účtu a rizika jejich zneužití. Člověk je čím dál vynalézavější, počet a forma útoků na bankovní data a tím pádem na peníze klientů se stále zvyšují, proto je potřeba s touto situací něco dělat, jak na rovině právní, tak i praktické.

Pro svou diplomovou práci jsem čerpal především z knižní literatury, internetových článků a aktuálních právních předpisů českých i evropských. Právě kvůli aktuálnosti této problematiky považuji elektronické zdroje za velmi důležité.

---

[1] Další používané označení pro elektronické bankovnictví: electronic banking, e-banking, direct banking či příme bankovnictví.

[2] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* rady a tipy. Praha: Computer press, 2000. 1/165 s. ISBN 80-7226-328-5

Pro hlubší pochopení jsem se zabýval nejen právní odbornou literaturou, ale také související literaturou z mimoprávních odvětví.

Pojem „elektronický“ je ve většině případů zaměňován s pojmem „internetový“, ten je potřeba chápat jako podřazený pojmu „internetový“, neboť v podstatě internetové systémy jsou zároveň i elektronickými. Vzhledem k této vazbě můžeme říci, že co se týká základní charakteristiky a zejména právní úpravy, platí pro oba systémy téměř to samé.

Cílem práce je seznámení se s pojmem elektronického bankovnictví jako celku, především vymezením produktů, jejich vlastnostmi, srovnáním, právní úpravou či možností jejich zneužití.

Práce, kterou drží čtenář v ruce je členěna do 6 kapitol, které jsou dále rozděleny do podkapitol, případně oddílů.

První část následující po úvodu se zabývá charakteristikou druhů elektronického bankovnictví, jejich historií a postupným vývojem. Do kapitoly je také začleněno stručné vymezení kladných a záporných stránek jednotlivých produktů.

Třetí kapitola s názvem „Bezhotovostní platební styk“ pojednává o výměně informací o platebních transakcích mezi bankami, jak domácími, tak mezinárodními převážně prostřednictvím technologie SWIFT, které se poté hlouběji věnuje.

Další část se věnuje problematice, která dělá vrásky většině z nás. Popisuji v ní možné útoky na osobní data a po sléze na finanční prostředky z našich bankovních účtů. Bankovní podvody jsou velmi rozšířenou obavou ve světě elektronického bankovnictví, proto je potřeba je nebrat na lehkou váhu a učinit maximum k jejich omezení.

V páté kapitole pojednávám o nebankovních platebních systémech, které sice nespadají pod bankovní institut, ale nesou mnoho společných znaků a jsou na nich svým způsobem závislý. Větší pozornost věnuji síti PayPal v dalších podkapitolách, jako vlajkové lodi tohoto průmyslu.

Předposlední část zkoumá právní úpravu vybraných otázek bankovnictví, jako např. náležitosti bankovních institucí, především bankovní licence a podmínky pro jejich získání. Dále pojednává o právní úpravě platebního styku, elektronických peněz, bankovního dohledu a o ČNB jako centrální bance.

2 Druhy a vývoj elektronického bankovnictví

2.1 Platební karty

Rok 1914, byl pro elektronické bankovnictví zlomový. Kolébkou tohoto vynálezu byly Spojené státy americké. Právě v tomto roce firma Western Union Telegraph Company vynalézá debetní platební kartu, která umožňovala zákazníkům posílat telegrafy bez okamžitého placení. „Tyto papírové karty se staly mezi obchodníky velmi oblíbené (klient měl své pohodlí a obchodník zase větší útratu za služby, které nabízel).“[3] I když se tyto historické karty od těch dnešních výrazně lišily, lze je pokládat za počátek elektronického bankovnictví.

O pár let později společnost Air Travel Card vydala platební kartu určenou pro obchodní cestující v oblasti letecké dopravy. Karty byly papírové nebo plechové a používaly se obdobným způsobem jako dnes. Klient předložil kartu a podepsal účet, prodavač měl za úkol zkontrolovat platnost a porovnat podpis. Avšak mnohem známější v tomto oboru je společnost DinersClub International, která v roce 1950 vydala universální platební kartu, z počátku poskytující jen 200 vybraným klientům. Zakladatele této firmy Franka McNamara vedla k vytvoření platebních karet nepříjemná situace, spočívající v zapomenutí peněženky v restauraci. DinersClub uzavíral se svými členy úvěrové smlouvy, ti bezhotovostně platili v restauracích a jednou měsíčně jim DC posílal výpis transakcí, které musel člen do 14 dnů uhradit. Za jeden rok se klubové karty této společnosti rozšířily natolik, že ji vlastnilo přes 35 000 členů a přijímalo 285 restaurací.

Úspěchu DinersClubu si začaly všímat první banky, netrvalo dlouho a New Yorská Franklin National Bank vydává první bankovní platební kartu. Banka vydávala karty jen důvěryhodným klientům, s horním limitem a povinností splatit platbu do 30, 60 nebo 90 dnů (záleželo na typu smlouvy)[4].

Od této doby se s bankami používající platební karty roztrhl pytel, v roce 1954 jich bylo téměř sto. Avšak netrvalo dlouho a třetina bank tuto službu přestalo používat, kvůli nezkušenosti a velkým ztrátám, způsobených právě touto novou technologií. Banky okrádali, jak klienti, tak zaměstnanci, kteří odcizovali karty

[3] Historie platebních karet. z: *Wikipedia*: *otevřená encyklopedie* [online]. Wikimedia Foundation, 2001- [cit. 24.2.2012]. Dostupné z: http://cs.wikipedia.org/wiki/Historie_platebn%C3%ADch_karet

[4] SCHLOSSBERGER, O. SOLDÁNOVÁ, M. a kol.: *Platební styk*, 2. dopl. vydaní Praha.: Bankovní institut, 2007 . 24/435 s. ISBN 80-7265-072-6

přímo z výrobních pultů. Platili nimi většinou menší částky, které nepodléhaly telefonickému ověření a tím unikali a páchali trestnou činnost mnohem déle. Do problémů se dostala i tehdy největší gigant Bank of America s produktem BankAmericard, kterou také ničili vynalézaví podvodníci.

Bank of America se z manka dostávala několik let, a to odradilo velké množství konkurenčních bank. Ze ztráty je BOA[5] dostává až v roce 1962, kdy vykazuje zisk 12,7 mil. USD. Úspěch nenechal dlouho čekat konkurenci a ta v vznikla v podobě MasterCard. Původně známá jako MasterCharge, která byla vytvořeno z několika bank v Kalifornii, jako konkurence BankAmericard vydané Bank of America, ta se později stala známou jako Visa kreditní karty vydané společností Visa Inc.[6] Postupem času tyto karty začala akceptovat většina bank, nejen v Americe, ale i ve zbytku světa.

Potřeba automatizace, pohodlnosti a hlavně zvýšené ochrany měla za následek opravdovou revoluci v tehdy ještě neznaném e-bankingu. Počítačový magnát IBM poprvé aplikoval magnetický proužek na platební kartu, která dokázala nést informace o držiteli, ale zároveň byla přepisovatelná, jako např. zůstatek na kontě nebo informace o transakcích. Karta měla jako ochranné prvky podpisový řádek a kód PIN. Air Travel Card byla první společnost, která kartu s magnetickým proužkem vydává. Do 4 let magnetický proužek začalo používat 85% platebních karet.

K plnohodnotnosti platebních karet chyběl přístroj, který by sám vydával peníze, ušetřil tak mnoho času, jak pracovníkům bank, tak samotným klientům.
První bankovní automaty se objevují v roce 1967 ve Velké Británii, na jejich vývoji se podílí i britská tajná služba MI5[7]. Zprvu bankomaty fungovaly na principu mechanický válců, z nichž vycházely peníze, klient si však musel nejprve vyzvednout na přepážce plechový štítek a PIN, který současně a jednorázově použil při výběru hotovosti. To však ztrácelo na významu urychlení transakce, proto bylo nutné vyrobit plně automatický bankomat napojený na vnitřní informační systém. To se povedlo o 5 let později Lloyds Bank.

Moderní bankomat s vnitřním systémem začalo používat stále více bank, avšak systémy komunikovaly jen mezi bankomaty jednotlivých společností. V roce

[5] BOA - Bank of America- je mezinárodní banka sídlící v Charlotte v Severní Karolíně. Patří k „velké čtyřce“ hlavních bank USA.
[6] Historie platebních karet. z: *Wikipedia*: *otevřená encyklopedie* [online]. Wikimedia Foundation, 2001- [cit. 24.2.2012].
Dostupné z: http://cs.wikipedia.org/wiki/Historie_platebn%C3%ADch_karet
[7] MI5- "pětka"-kontrašpionážní, zpravodajská agentura Spojeného Království, založena 1905.

1982 vstupují na trh Cirrus International a Plus, kterým se povedlo propojit bankovní sítě 90% bankomatů v USA. V roce 1992 Plus odkoupila Visa a Cirrus odkoupil MasterCard. Od této doby se začaly karty vyvíjet do podoby, jaké známe dnes, čipové, vyrobené z odolného plastu tvrzeného karbohydronátem[8].

Podle mého názoru byla právě platební karta největším průkopníkem v rozvoji dalších odvětví elektronického bankovnictví, jež se vyvíjely postupně s rozmachem nových technologií. Tak jak se vyvíjelo internetové a telefonní spojení, vznikaly nové produkty jako např. Telefonní, GSM, JAVA, WAP, PDA a nebo internetové bankovnictví.

2.1.1 Druhy platebních karet

Platební karty tedy slouží k bezhotovostnímu platebnímu styku nebo výběru hotovosti. Každá karta musí obsahovat: označení vydavatele karty, jméno a příjmení klienta, číslo karty, datum splatnosti, CVC[9] a v neposlední řadě také záznam dat ve formě magnetického proužku, mikročipu nebo laserového záznamu[10].

2.1.1.1 Dle technologie

Karta s nanesenou magnetickou vrstvou, sloužící k záznamu a čtení požadované informace. Karta má omezenou kapacitu, která je daná délkou magnetické stopy a hustotou záznamu. Data jsou zapsána do třech stop na magnetický pásek umístěny na rubové straně karty. Dvě stopy slouží pro čtení a jedna pro zápis. První stopa je určena pro vnitrostátní i mezinárodní off-line i on-line použití, druhá stopa pro vnitrostátní i mezinárodní on-line použití, třetí stopa pouze pro vnitrostátní off-line použití. Karta vybavená pouze magnetickým proužkem je velmi jednoduchá, bez vlastní inteligence s nejnižším stupněm ochrany, protože mnohdy jediným ověřením oprávněnosti k provedení transakce je pouhý, lehce napodobitelný podpis, a to vede ke snadné možnosti zkopírování

[8] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Platební karty. Praha: Computer press, 2000. 11/165 s. ISBN 80-7226-328-5

[9] CVC- bezpečnostní kód, trojmístné číslo nacházející se na zadní straně karty nad podpisovým proužkem.

[10] DVOŘÁK, P. *Bankovnictví pro bankéře a klienty*. 3. rozšířené vydání. Praha: Linde, 2005, s.371, ISBN 80-7201-515-X

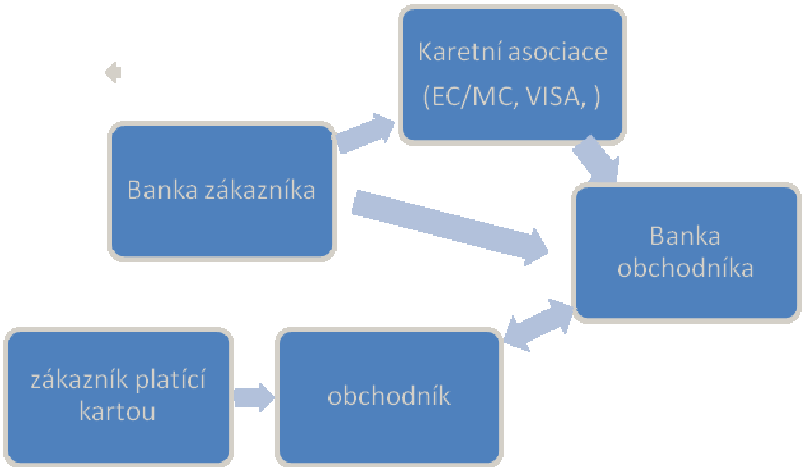
citlivých dat[11]. Tato technologie je dnes považována za zastaralou a v bankovnictví používána jen zřídka.

Inteligentní čipové karty jsou mnohem vyspělejší, obsahují procesorový kontaktní nebo bezkontaktní čip, jako nositele informace. Karta může obsahovat paměť různých typů, jako např. RAM, ROM, EPROM[12], díky kterým je možné na kartu nahrát větší množství informací, týkajících se držitele platební karty. Čipové karty snižují riziko zneužití neoprávněnou osobou nebo padělání, Celkově po zavedení čipových karet, v některých státech klesla až pětkrát trestná činnost páchaná zneužitím platebních karet.

Dnes již je Česká republika kompletně čipová a v placení platebními kartami patří ČR mezi nejbezpečnější v EU.

Pro nás jsou však nejznámější karty hybridní. Jde o technologii, kterou upřednostňuje většina společností a vznikla kvůli nedostatečnému pokrytí čipových terminálů. Karty jsou vybaveny jak magnetickým proužkem, tak procesorovým čipem, nemusíme se tedy strachovat jakého typu je dané snímací zařízení. Díky svému neomezenému použití, ale i vysoké ochraně se hybridní karty staly nejrozšířenější.

Všechny druhy karet musí vyhovovat mezinárodním standardům, stanoveny normou ISO 3554. Mají rozměr: 85,6 x 54,0 x 0,76 mm.



Obrázek 1: Vztah karetní asociace, obchodníka a bank[13]

[11] Tzv. skimming nebo-li skimmovací zařízení- Je technologie nebo přístroj, který dokáže přečíst data z magnetických platebních karet a buďto je zaznamenat do paměti nebo je následně posílá (např. formou SMS) pachateli.

[12] EPROM. z: *Wikipedia*: *otevřená encyklopedie* [online]. Wikimedia Foundation, 2001- [cit. 24.2.2012]. Dostupné z: WWW: http://cs.wikipedia.org/wiki/EPROM.

[13] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Platební karty. Praha: Computer press, 2000. 16/165 s. ISBN 80-7226-328-5

2.1.1.2 Dle způsobu zúčtování

Ne všechny karty jsou stejné. Dle zúčtovacího způsobu rozdělujeme platební karty na debetní a kreditní.

Debetní karty jsou napojeny přímo na Váš bankovní účet, můžete je použít k výběru hotovosti či nákupu zboží. Při použití bankomatu nebo platby za zboží či služby budete muset zadat PIN[14]a v některých případech se budete muset podepsat. K použití této karty je důležité mít nastaven dostatečný zůstatek a vyhovující limit. K této službě je možné si sjednat tzv. kontokorent, to znamená, že držitel může po vyčerpání svých prostředků využít prostředků banky a v určité době a s určitým úrokem jej splatit. Debetní karty jsou v současné době nabízeny ke všem běžným účtům, jsou velmi výhodné především pro banku samou, protože klient využívá převážně svých vlastních prostředků a banka tak nemusí vystavovat nebezpečí vlastní peníze.

V České republice se nesprávně vžil pojem „kreditní karta“ nebo-li „kreditka“. Ve většině případech ji přisuzujeme vlastnosti debetní karty. Rozdíl je především v tom, že kreditní karty jsou karty úvěrové, mohou být vystaveny bez běžného účtu. Držitel může pomocí této karty vybírat hotovost, platit za zboží a služby do výše sjednaného limitu. I když se tyto karty zdají výhodné, opak je pravdou. U většiny bank a spořitelen existuje možnost splatit do 45 dnů bezúročně. Pokud do této doby klient nesplatí celý úvěr, banka si začne účtovat vysoké úroky z úvěru (17-20%). Některé banky si účtují roční poplatky jen za to, že kreditní kartu využíváte. Při zřizování je velmi důležité dopodrobna promyslet celou situaci, aby nevedla k zadlužení.

2.1.1.3 Podle způsobu provedení

Dle způsobu provedení rozlišujeme karty na embosované a elektronické. Embosovaná platební karta je taková karta, na které je reliéfně (vystouplým tiskem) uvedeno jméno majitele karty, číslo karty a platnost karty. Tuto kartu lze na rozdíl od elektronických platebních karet použít i k tzv. mechanickým transakcím, tedy transakcím uskutečněným prostřednictvím imprinterů, kterým se lidově říká „žehlička“. Ne každý obchodník totiž disponuje elektronickým platebním terminálem.

[14] PIN- Personal Identity Number, identifikátor, podle kterého je možné se autorizovat.

S embosovanou platební kartou tak máte možnost zaplatit i u těch obchodníků, kteří disponují pouze imprinterem, tzn. že se Vám možnost použití Vaší karty několikanásobně zvětší. Navíc bych rád ještě poznamenal, že s většinou embosovaných platebních karet jsou velmi často spojené ještě další tzv. doplňkové služby. Jedná se zejména o pojištění pro cesty do zahraničí, silniční asistence apod. Úroveň a rozsah těchto doplňkových služeb se samozřejmě liší dle typu platební karty a dle banky, která příslušnou kartu vydala[15]. Výhodou embosované karty je že, pokud nefunguje online spojení terminálu s bankou, je obchodník povinen použít mechanickou čtečku. Při poruše terminálu elektronickou kartou nezaplatíte.

Elektronické platební karty jsou v ČR nejrozšířenější. Patří sem VISA, Electron a Maestro. Tyto karty lze použít pouze pro online transakce, jako jsou výběry z bankomatů či platby u obchodníků. Výhody těchto karet jsou: vedení zdarma, nízké poplatky za blokaci ztracené karty, nulová možnost zneužití zablokované karty[16].

V posledních letech banky přišly s novým druhem platebních karet, a to kartou virtuální, která slouží pouze k nákupu na internetu. Karta není fyzicky hmatatelná, jde pouze o 16 místné číslo karty vytisknuté na papíře, s časovou platnosti a bezpečnostního kódu CVV2/CVC2. Osobní identifikační číslo PIN se k virtuální kartě nevydává.

2.1.2 Budoucnost platebních karet

Dnes si mnoha z nás ani neumí představit, jak by se platební karta mohla dále vyvinout. Sympatický lesklý vzhled s možností volby vlastního obrázku, čipy, magnetické proužky, ale opak je pravdou.

Maximální kapacita paměti takové karty je pouhých 64 kb, a to v dnešním světě výpočetní techniky žijící v Gygabitech a Terabitech je neviditelná položka. Již dnes existují bezdotykové karty, uplatňované především v dopravě. Lze je

[15] SKOK, P. Poradce pro platební karty. *Měšec.cz* [online], 2004, [cit. 26.2.2012]. Dostupné z : http://www.mesec.cz/poradna/platebni-karty-zima-2004/259/

[16] Platební karta: *Wikipedia*: *Otevřená encyklopedie* [online]. [cit. 20-3-2012]. Dostupné z: http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta

použít bez přímého zasunutí do čtecího zařízení. Ve vývoji je také projekt placení z karty na kartu, které by mělo být snadné jako dobíjení kreditu mobilního telefonu – jen musíte znát číslo karty příjemce peněz. Východní Asie je v zavádění karetních novinek nejdál. Automobilka Hyundai ke svým luxusním vozům dává automaticky kreditní kartu s pojištěním, která zároveň slouží jako zajišťovací mechanismus.[17] Otázkou je, zda-li by se tyto vymoženosti uplatnily i v elektronickém bankovnictví, kde na prvním místě je především bezpečnost a minimální zneužitelnost.

Ani bankomaty nezůstávají pozadu, horkou novinkou jsou snímače sítnic, ale v České republice se s tím zatím nesetkáte. Pokrok jde dál s dobou a klasické scény ze sci-fi filmů se nejspíše brzy stanou realitou.

2.2 Telefonní bankovnictví

I když dnes tato technologie není příliš oblíbená a po příchodu internetového bankovnictví „zastaralá“, pro svůj obrovský přínos pro bankovnictví, bych ji rád ve své práci uvedl.

Po platební kartě je telefonní bankovnictví dalším chronologickým následníkem elektronického bankovnictví, dočkalo se masovějšího rozšíření a jeho klienti mají přístup k zadáváním bankovních operací nebo správě svého účtu prostřednictvím telefonu. Na přelomu šedesátých a sedmdesátých let, kdy technologie prudce vstoupaly, cena techniky klesala, nastával zlom pro mnoho oborů lidské činnosti a také pro oblast bankovnictví. Za boom telefonního bankovnictví je považován rok 1989, kdy vznikla First Direct[18], průkopník phonebankingu.

Lidé si začali zvykat na nepřetržitý přístup k hotovosti pomocí bankomatů, později také k jiným službám. Ukázalo se, že osobní kontakt s bankéřem není pro řadu klientů důležitý, mnoho z nich preferuje stálou dostupnost služeb prostřednictvím moderních komunikačních kanálů[19].

---

[17] ZÁMEČNÍK, P. Budoucnost platebních karet začíná! *Měšec* [online]. 2003, [cit. 26.2.2012]. Dostupné z: http://www.mesec.cz/clanky/budoucnost-platebnech-karet-zacina/

[18] First Direct je první telefonická retailová banka. Vznikla v Velké Británii, s dvěma call centry. V roce 1992 se stala součástí HSBC.

[19] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Telefonní bankovnictví. Praha: Computer press, 2000. 40/165 s. ISBN 80-7226-328-5.

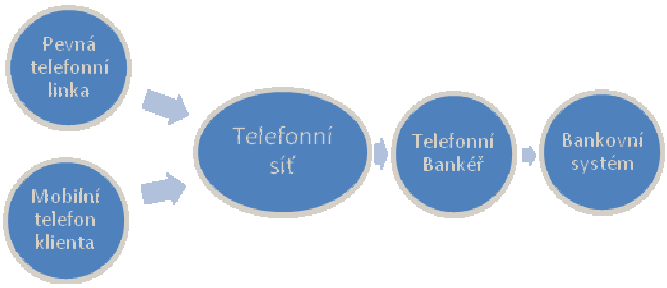
Pevná linka nebo mobilní telefon jsou nejdostupnějším komunikačním mediem. Před 10 lety neexistovaly chytré telefony s bankovními aplikacemi, nebylo ani tak dobré pokrytí sítě EDGE[20], 3G[21] nebo WIFI[22]. Lidé si museli vystačit pouze s klasickými nebo mobilními telefony.

Telefonní bankovnictví se samozřejmě historicky vyvíjelo a mnoho změn doznalo příchodem digitálních mobilních sítí[23], proto tuto kapitolu rozdělím na klasický phonebanking a GSM banking.

2.2.1 Klasický phonebanking

Telefonní bankovnictví je automatizovaný systém poskytovaný bankou za účelem přístupu k bankovním účtu pomocí telefonu. Tento systém umožňuje získat přístup k účtu a provést nezbytné operace. Jakmile vytočíte telefonní číslo banky, záznamník začne předčítat nabídku služeb a k nim přiřazené čísla. Stisknutím příslušného čísla na telefonu se dostanete do konkrétní nabídky.

Pomocí telefonu lze uskutečnit opravdu mnoho bankovních operací. Ovšem existují i složitější úkony, které i v dnešní době musí být vyřešeny osobně na pobočce, např. hypotéky.



Obrázek 2: Komunikace pomocí živého bankéře[24]

[20] EDGE- někdy také jako Enhanced Data rates for GSM Evolution je dalším vývojovým stupněm v technologií GSM
[21] 3G- je zkratka pro třetí generace mobilních telefonů. Služby spojené s touto generací představují schopnost přenášet hlasu i dat.
[22] WIFI- Wireless Ethernet Compatibility Aliance, bezdrátová síť.
[23] GSM- Globální Systém pro Mobilní komunikaci původně však francouzsky „Groupe Spécial Mobile“) je nejpopulárnější standard pro mobilní telefony na světě. GSM telefony používá přes miliardu lidí z více než 200 zemí. konkurence: WCDMA se používá hlavně ve Spojených státech a Kanadě.

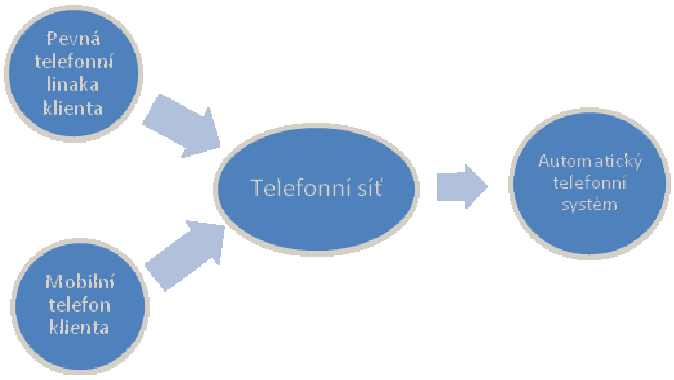
Operace prováděné po telefonu, a ne jen ty, lze rozdělit na několik úrovní, a to pasivní a aktivní. Obecně lze říci, že pasivní operace nemění stav účtu klienta, jedná se o sdělování veřejně dostupných informací o účtu, bance, produktech či zůstatku. Pasivní operace jsou mnohem jednodušší, u většiny bank jsou první fází. Jakmile je tato etapa úspěšně překonána, může nastoupit fáze druhá. Aktivní operace jsou technicky a bezpečnostně náročnější.

Pasivní operace	Aktivní operace
Zjištění zůstatku na účtu	**Příkazy k úhradě a inkasu**
Informace o pohybu na účtu	**Trvalé příkazy k inkasu**
Informace o zadaných transakcích	**Trvalé příkazy k úhradě**
Informace o produktech a službách	**Blokace účtu**
Úrokové služby	**Zahraniční platební styk**
Kurzovní lístek	**Správa terminovaného vkladu**

Tabulka 1: Aktivní a pasivní operace bank[25]

V blízké minulosti, kdy ještě komunikační technologie nebyly na úrovni jako dnes. Především díky absenci automatizace, si lidé pod pojmem telefonního bankovnictví představovali živého bankovního poradce sedícího v call centru. Nyní je situace trochu jiná, lidskou pracovní sílu ve většině bankovních operacích nahradil automatizovaný záznamník a pro bankéře zbylo jen vyřizování reklamací a jiných problémů, na které je IT stále krátká.

[24] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Telefonní bankovnictví. Praha: Computer press, 2000. 439/165 s. ISBN 80-7226-328-5.
[25] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Telefonní bankovnictví. Praha: Computer press, 2000. 41/165 s. ISBN 80-7226-328-5.



Obrázek 3: Komunikace s bankou pomocí automatického záznamníku[26]

Otázkou stále je, zda-li tento neosobní systém je sympatický pro klienty. Často se stává, že s robotickým záznamníkem nevyřešíte svůj problém, a tak Vám nezbývá nic jiného, než se stejně nechat přepojit na operátora. Mnoho bank si tuto skutečnost uvědomuje, a proto využívají oba tyto systémy. Automatický telefonní systém je prakticky nenáročný, k uskutečnění operace Vám postačí pouze telefon a trocha technické zdatnosti k zvládnutí tónové volby. Záznamníkový systém pracuje na základě menu, po kterém se pohybujete pomocí stisku čísel na telefonu. Největší výhodou tohoto systému je jeho nákladová nenáročnost, proto především pasivní operace jsou poskytovány zcela bezplatně.

2.2.1.1 Bezpečnost telefonního bankovnictví

Co se týče klientské ochrany, telefonní bankovnictví není zrovna bezpečný typ. Při osobní návštěvě pobočky banky, Vám bankéř může snadno zkontrolovat osobní doklady, taková možnost u tohoto typu neexistuje, proto banky hledají různé alternativy, které by zaručily bezpečnost a nezneužití peněz na účtu klienta.

Možností je více, míra složitosti a bezpečnosti se odvíjí od charakteru operace. Mezi nejjednodušší druhy zabezpečení, používané především pro pasivní operace, se často využívá osobního čísla klienta[27] a kódu PIN. Tento princip by se dal pochopitelně použít i na transakce, ale možnost zneužití je vysoká. V praxi se používá především dvouúrovňový systém, který je kombinací předchozího, tedy osobního čísla a PIN s jednorázovým heslem, které získá většinou při aktivaci

[26] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Telefonní bankovnictví. Praha: Computer press, 2000. 42/165 s. ISBN 80-7226-328-5.
[27] Osobní číslo klienta - identifikuje klienta jako osobní číslo se často používá i číslo účtu.

telefonní bankovnictví. Klient jednorázových hesel obdrží několik podle typu banky, většinou však dvacet nebo padesát. Po autorizaci operace heslo ztrácí význam a na další úkon je potřeba hesla nového.

Další podpůrné bezpečnostní systémy jsou např. limit pro telefonní transakci, měsíční obměna kódu PIN, monitorovaný hovor s bankéřem nebo zablokování vstupu po třikrát špatně zadaném PIN.

Bankovnictví pomocí telefonického spojení bylo na výsluní v letech 2000 až 2004. Po příchodu internetového a GSM bankovnictví, to telefonické rychle upadlo. Dnes se převážně využívá k informacím a prodeji produktů, řešení jednoduchých problémů nebo blokaci účtu.

2.2.2 GSM bankovnictví

Tento typ bankovnictví se rozšířil díky stále větší expanzi trhu mobilních telefonů. Dnes vlastní mobilní telefon téměř každý z nás, máme ho neustále při sobě, a to z něj dělá nejdokonalejší medium pro aplikaci bankovnictví kdekoliv na světě. Klient má možnost spravovat svůj účet pohodlně ze svého mobilního telefonu, kdykoliv potřebuje, aniž by navštívil pobočku banky.

Do mobilního bankovnictví by jsme dnes mohli zařadit i klasické telefonní bankovnictví, tedy komunikaci klienta s operátorem v call centru nebo s automatickým záznamníkem (IVR)[28], dále GSM SIM Toolkit, SMS banking, WAP banking.

2.2.2.1 SMS banking

Mezi chronologicky první GSM službu můžeme považovat právě SMS banking. Tato technologie poskytovaná bankou, je založená na komunikaci prostřednictvím SMS push & pull zpráv, které umožňují poskytovat vybrané bankovní služby přes mobilní telefony.

[28] IVR- Interaktivní hlasová odezva. Systém využívaný v telekomunikačních službách, určený ke komunikaci se zákazníkem. Při složitých otázkách, následuje připojení na operátora.

Push zprávy jsou ty, které se banka rozhodne vyslat na zákazníkův telefon, k jejichž odeslání klient nežádal. Tyto oznámení mají především podobu zpráv marketingových nebo upozorňujících na události o pohybu na účtu. Dalším typem push zpráv je jednorázové heslo, tzv. OTP[29], které je posledním nástrojem k boji proti bankovním podvodům. Pokaždé, kdy klient chce provést transakci pomocí mobilního nebo internetového bankovnictví, OTP je mu zasláno pomocí SMS zprávy na jeho telefon. Heslo je vygenerováno pouze pro konkrétní úkon a na určitou dobu, poté ztrácí platnosti. Zákazník je oprávněn si vybrat ze seznamu nabízených upozornění, které chce odebírat.

Pull zprávy, jsou ty, které jsou iniciovány ze strany zákazníka, Pokud si pamatujete strukturu předdefinované SMS, odešlete ji na konkrétní číslo banky, tím jí přikážete proces, který má splnit a ona též ve formě SMS odpoví. Tato možnost je relativně snadná, ale mít stále na paměti tvar zprávy a podobu správných výrazů občas bývá limitující faktor. V tabulce zobrazené níže jsem shrnul operace, které lze docílit touto technologií.

PUSH	PULL
Pravidelné informace o zůstatku na účtu	**Dotaz na zůstatek na účtu**
Informace o (ne)vyřízení transakce	**Dotaz na úrokové sazby**
Nedostatek finančních prostředků	**Dotaz na kurz měn**
Velké hodnoty na účtu	**Deaktivace platebních karet**
Velké hodnoty výběru z bankomatu **Velké hodnoty platby platební k.**	**Převod peněz mezi vlastními účty klienta**
Jednorázové heslo	**Mini výpis účtu**

Tabulka č. 2: Srovnání push & pull zpráv[30]

Dnes je tento způsob sdělování informací podporován jak ve formě SMS, tak i elektronickou poštou a bývá často zpoplatněn nemalými částkami. Druhá, mnohem přívětivější možnost je softwarové rozhraní GSM SIM Toolkit.

[29] OTP- One Time Pasword, v překladu jednorázové heslo
[30] Zdroj: http://www.easysoftware.cz/pull-x-push-marketing-nebo-kombinace

2.2.2.2 SIM Toolkit

Společnost RadioMobil, která před lety provozovala síť mobilních telefonů Paegas byla v roce 1998 společně s Expandia bankou jednou z prvních společností na světě, které bankovní aplikaci GSM SIM Toolkit uvedla do komerčního použití. O světovém významu českého řešení Paegas SIM Toolkit svědčí i mezinárodní ocenění. První na mezinárodním fóru Global Mobile Commerce (GMCF) v Londýně a druhé na konferenci operátorů GSM v Cannes.[31]

Systém je založen na kooperaci banky a mobilního operátora, která v minulosti nebyla tak samozřejmá jako dnes. Vybrané banky nespolupracovaly s některými operátory. Pokud tedy potencionální klient měl zájem o tento produkt, musel si svůj krok důmyslně promyslet, aby mu vyhovovala, jak banka, tak mobilní operátor. Dnes je situace mnohem příznivější, SIM Toolkit podporují všichni mobilní operátoři s většinou bank působící v ČR.

Na samém počátku této služby bylo za potřebí speciální SIM karty, kterou Vám operátor vyměnil a na pobočce banky jste ji museli aktivovat. Tím došlo k propojení obou společností a aktivaci služby. Změna SIM karty byla nutná kvůli menu telefonu, ve kterém přibyla položka SIM Toolkit, ze které se tato služba ovládala. Dnes je tomu jinak, informační technologie jsou na vysoké úrovni a SIM karty se programují na dálku. Přesná struktura menu se liší podle zvoleného peněžního ústavu. Po rozšíření nabídky máte možnost ze svého mobilu kontrolovat stav účtu, provádět transakce nebo využívat další služby.

Bezpečnost tohoto systému je založena na dvojici čísel, jsou to BPUK a BPIN. Bankovní PUK získáte v bance při aktivaci služby, pomocí něj si vytvoříte BPIN, který pak používáte při každé bankovní operaci. Oba kódy se chovají, tak jak je známe z použití u SIM karet mobilních operátorů. Po třikrát špatně zadaném BPIN se aplikace zablokuje a je vyžadován BPUK. Pokud zadáte desetkrát špatně bankovní PUK, SIM karta se zablokuje a už ji nelze pro bankovní služby použít.

Na vývoj mobilní komunikace v oblasti bankovnictví je kladen velký důraz. Mobilní telefony se stále vyvíjejí, jejich výkony dosahují výkonu počítačů a prakticky lze na nich provádět ty samé úkony. Síla mobilních procesorů, dotykové displeje, paměť měřená v GB[32] téměř všude dostupné pokrytí internetové sítě, to

[31] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Mobilní komunikace mění celý svět.. Praha: Computer press, 2000. 56/165 s. ISBN 80-7226-328-5.

[32] GB- Gygabyte, byte je jednotka množství dat v informatice.

jsou faktory, které mají největší vliv na vývoj mobilního bankovnictví, které známe dnes. Ani vývoj GSM SIM Toolkit se nezastavil a s příchodem technologie WAP[33], se začal provozovat také na její platformě.

2.2.2.3 WAP banking

Tento druh bankovnictví leží na pomezí GSM a internetového bankovnictví. Připojení k internetu přes WAP, je jakousi omezenou verzí dnešních plnohodnotných mobilních prohlížečů, které jej také plně nahradily a dnes se vyskytuje jen ojediněle. Rozdíl je především v zobrazení, zatímco webové prohlížeče se zobrazují na velkých obrazovkách počítače, WAP je určen k výstupu na malé displeje mobilních telefonů, u kterých se soustředí především na textové informace.

První, kdo zpřístupnil tyto služby, byla v roce 2000 Expandia Banka. K zajištění bezpečnosti používala elektronický klíč[34]. Použitím mobilního telefonu a elektronického klíče bylo možné kontrolovat stav účtu, provádět transakce, zřizovat termínované vklady nebo zjišťovat aktuální kurzy měn.

Paradox je, že při boomu WAP technologie byl kladen důraz na technologický vývoj mobilních telefonů, většina jich WAP nepodporovala, protože to prostě neuměla. Dnes je situace ve své podstatě stejná, moderní telefony také neví, co je WAP, a to z důvodu, že ho prostě nechtějí podporovat a po příchodu plnohodnotného internetu v mobilním telefonu tu zastaralou technologii ani nepotřebují.

2.3 Homebanking

PC bankovnictví je také určitý druh komunikace mezi zákazníkem a bankovní institucí pomocí bankovního programu, dodávaného bankou a nahranou právě ve vašem PC. Přenos dat je obousměrný, jak od klienta k bance, tak z banky ke klientovi a je uskutečněn pomocí datových sítí.

---

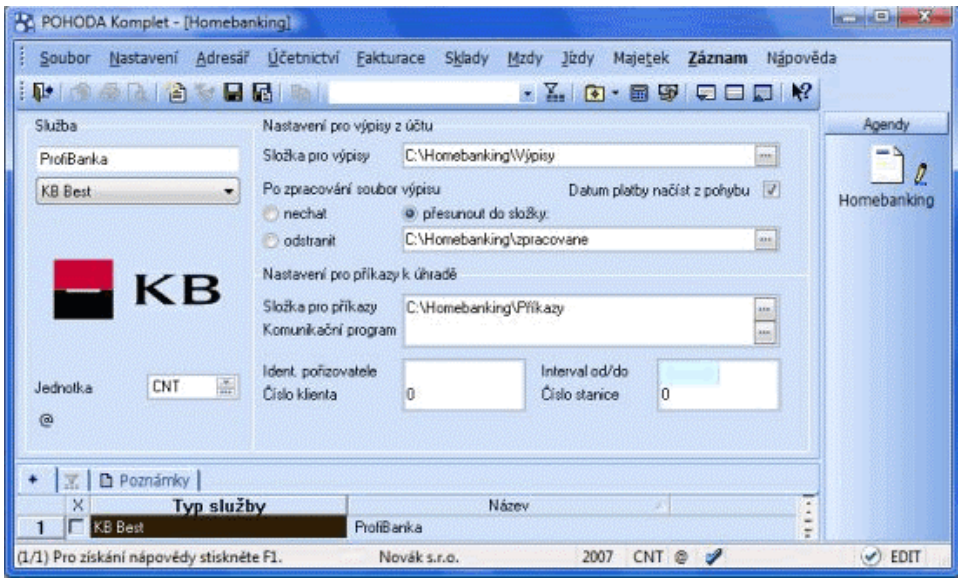
[33] WAP- Wireless Application Protocol, systém pro zajištění elektronických služeb na mobilních telefonech.

[34] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Mobilní komunikace mění celý svět.. Praha: Computer press, 2000. 59/165 s. ISBN 80-7226-328-5.

Cesta vývoje byla v jádru jednoduchá, homebanking vznikl převážně díky náročnosti velkých firem, které prakticky denně na pobočce banky vyplňovaly desítky formulářů, které časově tížily, jak banku, tak samotné klienty. K vytvoření PC bankovnictví banky popohnaly právě chytré účetní programy, které dokázaly vytisknout konkrétní bankovní formuláře, se kterými firemní klienti chodili na přepážky a pracovníci banky je museli přepsat do systému. Tento způsob byl ulehčením pouze pro klienty a s tím banka musela něco dělat.

Banky se situaci snažily řešit. Z počátku homebankingu, začaly poskytovat velkým firmám programy, pomocí kterých si na počítači vyplnili formuláře v potřebné kvantitě, poté je přesunuli na určité médium, v té době to byly diskety a přenesly na pobočku banky, kde informace z diskety zkopírovali a pomocí vlastnoručního podpisu transakce autorizovali. Tento způsob sice zvládal hromadné operace, ale stále bylo zapotřebí lidské přítomnosti na obou stranách.
Tímto způsobem si banky ověřily, že lze elektronicky vyplnit formulář a že je o tento systém velký zájem. Bankám tedy chyběl ten poslední krůček k tomu, aby umožnily klientům vyplňovat příkazy z pohodlí svého domova či kanceláře a pomocí komunikačního kanálu je poslali bance bez fyzické přítomnosti na pobočce.

První homebankingové programy fungovaly na semi online bázy, které se připojovaly přes internet k bankovnímu systému jen několikrát denně v určitou hodinu, za účelem odeslání dat. Netrvalo však dlouho a PC bankovnictví se vyvinulo do zcela online formy, kde klient může zadávat příkazy 24 hodin denně, které se ihned odesílají. Tento druh bankovnictví je jeden z nejstarších druhů přímého bankovnictví, které nabízí aktivní prvky pomocí PC napojeného na systém banky. Homebanking často veřejnosti splývá s internetovým bankovnictvím. Rozdíl je především v nutnosti počítače, připojení k internetu a hlavně speciálního programu, který Vám musí poskytnout banka. U Internetového bankovnictví stačí mít připojení k internetu a přístroj s integrovaným prohlížečem, jako je počítač, tablet, mobilní telefon a dnes už také televizor.



Obrázek 4: Program Pohoda, Homebanking od KB[35]

Výhodou této bankovní aplikace je výborný přehled o historii účtu, zadávání bezhotovostních transakcí, také vysoce užitečná manipulace s bankovními daty a vysoká kompabilita s různými účetními programy, což usnadní práci nejedné firmě. Klient může data přímo importovat do účetního programu a naopak, platební příkazy přímo zadávat do konkrétního účetní aplikace. V tomto ohledu je PC bankovnictví ojedinělé a nenahraditelné.

O homebakingových programech různých bank lze říci, že pracují a také vypadají velmi podobně, liší se jen nepatrně, což je v dnešním konkurenčním boji logické. Banka při vývoji programu klade velký důraz především na způsob komunikace se serverem, nenáročné ovládání aplikace, celkovou funkčnost a v neposlední řadě bezpečnost.

Právě homebanking se může pochlubit s jedním z nejlepších zabezpečovacích systémů v elektronickém bankovnictví probíhající přes kódované kanály. Před provedením aktivní operace, je třeba se náležitě přihlásit, a to pomocí hesla a autorizačního certifikátu. Oprávněnost osoby hraje velikou roli, některé homebankigové programy umožňují, aby některé příkazy mohla připravit neautorizovaná osoba např. sekretářka nebo účetní a rovnou je mohla poslat do banky. Banka však příkazy neprovede do doby, než je nepotvrdí certifikovaná osoba např. ředitel společnosti[36].

[35] DOBEŠ, Pavel. Pohoda 2008. *Programy* [online]. 2008 [cit. 27-3-2012]. Dostupné z: http://www.swmag.cz/assets/clanky/2008-03/clanek00213/upload/photo/Homebanking.png

[36] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* kap. Mobilní komunikace mění celý svět.. Praha: Computer press, 2000. 77/165 s. ISBN 80-7226-328-5.

Jak kooperace s účetními programy, tak autorizace na dálku jsou předními atributy PC bankovnictví, ale i přes to jsou u fyzických osob a menších podniků nahrazovány bankovnictvím internetovým. V praxi ani mnohdy nenajdeme takové rozdíly mezi těmito druhy elektronického bankovnictví, až na potřebu softwarové aplikace takřka splývají. Proto bych v neposlední řadě napsal pár slov k bankovnictví internetovému.

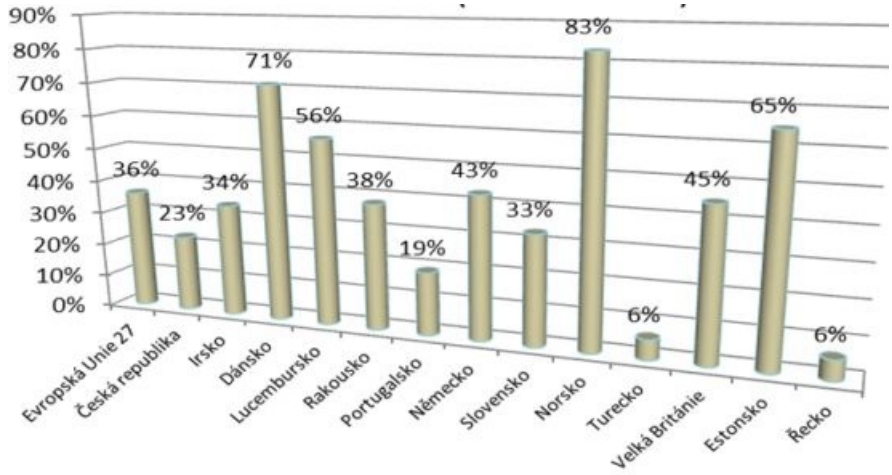
2.4 Internet banking

Příchod internetu urychlil vývoj nejen nových průmyslových odvětví, ale změnil i sektor obchodní, a to především bankovnictví. V roce 1995 vznikla první internetová banka Security First Network Bank. Přibližně ve stejnou dobu Wells Fargo jako první banka z cihel a malty zavedla produkt internetového bankovnictví. Než se internetové bankovnictví dostalo do podoby, jakou známe dnes, mělo vzhled firemní webové stránky. Banky brzy začaly vyvíjet webové aplikace, které na začátku pouze umožňovaly přístup k jejich účtům a až později se vyvinuly k možnosti provádění finančních operací online. V roce 1998 první, kdo v ČR představil internetové bankovnictví byla družstevní záložna FIO. Avšak většího rozmachu se této technologii dostalo až o rok později, kdy ho spustila Expandia banka. Tím se otevřely dveře i ostatním bankám. Vývoj na sebe nenechal čekat a po roce 2002 bylo internetové bankovnictví samozřejmostí.

Internet banking umožňuje klientům banky spravovat svůj účet pouze přes webové stránky na internetové síti. Není k němu potřeba žádné speciální bankovní aplikace, jako je tomu u Home bankingu. Stačí zadat webovou adresu, náležitě se přihlásit a začít provádět operace. Můžeme být třeba na druhém konci světa, stačí nám pouze připojení k internetu a přístroj, přes který se připojíme. Dnes je zcela běžné provádění bankovních operací přes internet pomocí počítače, mobilního telefonu, ale i tabletu nebo televizoru. I webových prohlížečů vhodných pro tento typ bankovnictví je nemalá řada, jsou to např. Internet Explorer, Mozilla Firefox, Opera, Google Chrome atd.

Internet banking je nejoblíbenější bankovní produkt vůbec. Nejvíce využívaný je především v zemích EU, kde ho využívá až 36% klientů. Naopak státy bývalého východního bloku, které mají převážně ekonomický problém sami se

sebou, využívají internetové bankovnictví jen zřídka. Z postkomunistických států je v nejmenší oblibě v Rumunsku nebo v Bulharsku, kde je využit pouhými 2% klientů. Ale ani v Řecku internetové bankovnictví nepatří mezi oblíbenou službu, využívá ho tam pouhých 6% bankovních klientů. Největšího rozmachu se internet banking u těchto států projevil v roce 2003, kdy se zvedl z pouhého jednoho procenta užívání a pomalu se stále zvedá dál.



Graf 1: Využívání internetového bankovnictví ve světě v roce 2011[37]

Naopak, jak můžeme vidět v grafu č.2 se této službě daří především státům s vyspělým bankovnictvím vůbec a také státům severským. Největším boom od roku 2003 zaznamenalo Dánsko, které se zvedlo z hodnoty 38% až na dnešních 71% uživatelů. Velmi dobře s užíváním internetového bankovnictví jsou na tom také Finsko, Švédsko nebo Island, kde se hodnota využití přesahuje 75%. Nejvyspělejší stát, co do využívání internetového bankovnictví, je podle Eurostatu Norsko, kde využívá internet při bankovních operací přes 83% klientů bank a to je opravdu vysoké číslo.

Důvod takového rozdílu využívaní internetové bankovnictví u jednotlivých států je dán především úrovní pokrytí 3G[38] sítě a pokrytí klasického internetu obecně. V severských státech pokrytí připojení domácností a firem k internetu přes 3G dosahuje 70 %. Jen pro srovnání státy jako: Řecko, Bulharsku nebo

[37] Www.eurostat.ec: Využívání internetového bankovnictví ve světě: věk 16-74 let. [online]. 2011
[38] 3G - je označení 3. generace mobilních sítí, umožňující vysokorychlostní přenos dat.

Rumunsku nepřesahují svým pokrytím 3G sítí 9%. V České republice tato hodnota také není příliš vysoká, je spíše pod průměrem a činní 19% pokrytí[39].

Přece jen při použití internetové bankovnictví jde jen o Vaše peníze, proto bezpečnost toho druhu musí být na nejvyšší úrovni. Zabezpečení není jednotné, je rozdělené do více sekvencí, které jsou na sobě závislé a při absenci alespoň jednoho z nich, bezpečností systém neprovede zadanou operaci. Je logické, že stupeň bezpečnosti je u různých bank různý. První fáze zabezpečení začíná již přihlášením do systému, kde je nutno zadat buď Vaše ID číslo, certifikát nebo elektronický klíč a to vše v kombinaci se silným heslem.

Banky doporučují mít certifikát uložen mimo PC, např. na CD, USB flash nebo v nejlepším případě na čipové kartě, ke které je ale potřebná zabudovaná čtečka takových karet. Při provádění aktivních operací, se o bezpečnou autorizaci banka stará tak. že zasílá zabezpečené SMS s jednorázovými hesly. Některé banky pro autorizaci transakce či jiných operací na účtu využívají kódu z TAN[40].

K ještě vyššímu stupni bezpečnosti banky využívají doplňkové služby, jsou to grafické klávesnice, snadná možnost změny hesla, volba limitů nebo oznamovací SMS.

Tyto služby se na první pohled zdají, že jsou naprosto neprolomitelné, ale jsme jen lidi a největší nepřítel zabezpečovacích bankovních systémů je sám člověk. Především uživatel by měl dbát na bezpečnostní opatření doporučené bankou, spočívající především v ochraně bezpečnostních údajů. Banky především varují, aby klient zásadně nikomu nesděloval informace o účtu, ani rodinným příslušníkům, dále velmi nebezpečný faktor je používání veřejných počítačů, např. internetové kavárně, ke kterým má přístup prakticky každý. Existuje mnoho škodlivých programů, které dokážou uložit citlivá data, které pak zločinecké organizace na druhé straně světa moc rády využijí viz. další kapitola.

3 Bezhotovostní platební styk

[39] ROTTOVÁ, S. Jak moc se používá internetové bankovnictví ve světě. *Www.finance.cz* [online]. 2011 [cit. 3.3.2012]. Dostupné z: http://www.finance.cz/zpravy/finance/319968-jak-moc-se-pouziva-internetove-bankovnictvi-ve-svete-/

[40] TAN - tabulka autorizačních čísel, je poskytována bankou v počtu 20 nebo 50 jednorázových hesel.

Zprostředkování bezhotovostního platebního styku spočívá ve výměně informací o platebních transakcích mezi bankami, jak domácími, tak mezinárodními. Je to platební styk uskutečňující se mezi bankovními účty, uvěrovými účty nebo prostřednictvím směnek. Masa přenášených citlivých dat podléhá nejvyšší ochraně proti zneužití a úniku. Velký důraz je také kladen na rychlost a kvantitu přenosu datových zpráv, která u větších bank dosahuje i několik tisíc položek denně[41].

3.1 S.W.I.F.T.

První technologií pro přenos dat v platebním styku mezi bankami byl dálnopis[42], dnes je převážně ve vyspělých zemích nahrazen mezinárodní telekomunikační sítí S.W.I.F.T.

Dálnopis byl používán především menšími bankami, které nezpracovávaly příliš velký počet platebních operací a použití swiftové sítě pro ně bylo příliš nákladné. I dnes stále existují státy, kde se přenos dat pomocí S.W.I.F.T. nevyskytuje a jediný důvod, jak přenést bankovní informace je právě dálnopis. Jsou to státy Středního a Dálného Východu. Taková situace pochopitelně nutí vyspělé banky, aby v těchto situacích používaly dálnopisného spojení.

Pod symboly S.W.I.F.T. se skrývá název Společnosti pro mezibankovní finanční telekomunikaci[43]. Její činnost spočívá ve spojování bank a jiných finančních institucí prostřednictví telekomunikační sítě a zajišťuje rychlý a bezpečný přenos finančních transakcí.

3.2 Rozvoj a přednosti S.W.I.F.T.

Na konci šedesátých let, při růstu mezinárodních transakcí, které převyšovaly lidské možnosti manuálního zpracování, tak bankovní instituce komunikovaly

[41] SCHLOSSBERGER, O. SOLDÁNOVÁ, M. a kol.: *Platební styk*, Praha.: Bankovní institut, 2007. 285/435 s. ISBN 80-7265-072-6

[42] Dálnopis nebo-li Telex je telekomunikační zařízení umožňující bezobslužný datový přenos textových zpráv po speciálních nebo i telefonních linkách.

[43] S.W.I.F.T. tato zkratka přesně zní: The Society for Worldwide Interbank Financial Telecomunication.

především pomocí telexu, který nenabízel bezpečný přenos ani možnost pro rozvoj. Náklady dálnopisu stále stoupaly a banky byly nuceny k vytváření vlastních zúčtovacích systémů. Právě různorodost těchto systému, vysoké náklady a rozdílný jazyk vedli ke komplikaci. Poptávka rostla po jednotném mezinárodním telekomunikačním systému. V České republice byl dálnopis zrušen v roce 2008. Pro telekomunikační síť byl nejvýznamnější rok 1973, právě v květnu téhož roku skupina 239 bank z Evropy a Ameriky založila neziskovou organizaci ve vlastnictví členských bank. Úkolem této společnosti bylo sjednocení mezibankovní komunikace a umožnění přenosu dat. Zdokonalování systému trvalo až do roku 1977, kdy byl jeho vývoj dokončen a uveden do provozu. Ještě před spuštěním počet členských institucí vzrostl na 586. První zprávu, která přes SWIFT proběhla uskutečnil Princ Albert, král Belgie. Provoz již v prvním roce překonal všechna očekávání, bylo přes něj odesláno 3,4 mil. zpráv s denní odesílací frekvencí přesahující 300 000 swiftových zpráv.

ROK	POČET ZEMÍ	UŽIVATELÉ	OBJEM ZPRÁV V MIL.
1977	**22**	**518**	**3.4**
1980	**36**	**768**	**46.9**
1985	**58**	**1946**	**157.2**
1990	**83**	**3049**	**332.9**
1995	**137**	**5229**	**603**
2000	**192**	**7125**	**1274**
2003	**200**	**7527**	**1817**

Tabulka 3: Vývoj swiftové sítě od roku 1977 do 2003

Této síti hrála do not především její potřeba pro světové bankovnictví, její mezinárodní rozsah spojoval již na konci roku 2003 přes 7500 bank z 200 Států. Právě systémová adaptibilita, která vychází vstříc standardům swiftových zpráv, díky ním jsou data přenášena, ale také bezhotovostnímu platebnímu styku uskutečňovaného pomocí otevřených účtů[44].

[44] Nostro a loro účty (z lat. *nostro* = náš, *loro* = Váš), jsou korespondenční účty, které se především používají k mezinárodnímu platebnímu styku.

Swift také položil základní kámen pro platební systém evropské měnové unie, zvaný TARGET[45].

SWIFT je společností spojován většinou ve spojení s mezinárodním platebním stykem, ale banky je mohou a také využívají pro národní transakce, většinou pro interní mezi pobočkami a centrálou nebo pobočkami navzájem.

Můžeme tedy říci, že mezi přednosti SWIFT patří zejména minimalizace rizika přenášených zpráv a minimální náklady, to vše vede k celkové efektivitě a zvýšení produktivity při přenosu finančních informací. Jak už jsem psal výše, družstevní společnost SWIFT je ve vlastnictví bank, které se sami účastní této telekomunikační sítě. Tento systém neslouží pouze k přenosu platebního styku, ale také přenosu dat, nesoucích informace z finančních transakcí z peněžního a kapitálového trhu. Z počátku data z platebního styku tvořily většinu celkového přenosu, ale dnes postupně dochází ke snižování podílu v oblasti platebního styku, který tvoří pouze kolem 50% celkového přenosu informací SWIFT a do popředí se pomalu dostává oblast kapitálového trhu.

Swiftová síť je založena na dvojici operačních střediscích, jedno se nachází v Evropě a druhé v USA. Tyto základny jsou na sebe napojeny a tvoří jeden záložní celek na ukládání dat. V případě poruchy jednoho střediska, funkci přebírá druhé a naopak. Nedílnou součástí této koncepce jsou tzv. národní koncentrátory, které slouží jako regionální zpracovatelé pro jednotlivé členské státy.

3.3 SWIFT v České republice

ČSOB se jako první banka východní Evropy stala v roce 1981 členem družstevní společnosti SWIFT a svou první zprávu přes tento systém odeslala v roce 1983. Poté k připojení následovaly: v roce 1989 Živnostenská banka a o dva roky později Komerční banka spolu s Investiční bankou. Po roce 1992 se swiftová komunita rozšířila o dalších deset členů a začal v této oblasti boom. Přenos swiftových se zpráv v roce 1992 zrost o 69% oproti roku předchozímu a spojovací procesor umístěný v ČSOB byl technicky na kraji kolapsu. Proto společnost musela posílit spojovací server a podepsala smlouvu se společností Eurotel, která

[45] TARGET je eurový platební systém provozovaný centrálními bankami eurozóny, který byl uveden do provozu 1. ledna 1999. Tento platební systém se skládá z národních platebních systému zemí EU, platebního mechanismu ECB a spojovacího mechanismu, který jednotlivé systémy propojuje v jeden velký integrovaný systém.

ho od listopadu 1992 začala poskytovat v Praze na Žižkově[46]. Největší české banky dnes v přenosu dosahují množství 10 000 zpráv, tedy přijatých i odeslaných mimo špičku.

3.4 Swiftová zpráva

Přenos dat v rámci swiftové sítě se uskutečňuje pomocí swiftových zpráv. Jsou založeny na vysokém stupni standardizace formy a obsahu. Komunikace je založena na společném jazyku, kterým je angličtina. Zabezpečení zpráv spočívá v jejich zakódování a vzájemné výměně kódových klíčů mezi bankami navzájem.

Jeden ze standardů, kterými zprávy disponují je mezinárodně platné rozlišení podle jednotlivých kategorií. Každá swiftová zpráva obsahuje písmena MT a tři numerické znaky:

MT x y z

x = kategorie zprávy

y = skupina zprávy

z = typ zprávy[47]

Skupina „zprávy“ určuje funkci zpráv v dané kategorii. Typ zprávy specifikuje funkční detaily a kategorie zpráv označuje účel obchodu a člení se do 11 kategorií. Tyto kategorie se ještě zužují do podkategorií podle svého účelu:

- **systémové** - slouží k výměně informací swiftovou sítí a uživateli sítě v rámci technických aspektů. Spadají do kategorie MT 0.
- **finanční** - jsou určeny pouze k finančním transakcím mezi uživateli. Jsou zařazeny do kategorie MT 1-9.
- **služební** - technické zprávy, které slouží pro potvrzení zpráv či potvrzení systému.

[46] SCHLOSSBERGER, O. SOLDÁNOVÁ, M.: a kol.: *Platební styk*, Praha.: Bankovní institut, 2007. 292/435 s. ISBN 80-7265-072-6

[47] SCHLOSSBERGER, O. SOLDÁNOVÁ, M.: a kol.: *Platební styk*, Praha.: Bankovní institut, 2007. 293/435 s. ISBN 80-7265-072-6

KATEGORIE	ÚČEL
0	SYSTÉMOVÉ ZPRÁVY
1	ÚHRADY KLIENTŮ
2	MEZIBANKOVNÍ PŘEVODY
3	OPERACE NA PENĚŽNÍCH TRZÍCH
4	INKASA
5	OPERACE S CENNÝMI P.
6	DRAHÉ KOVY A KOMODITY
7	AKREDITIVY A ZÁRUKY
8	CESTOVNÍ ŠEKY
9	ZŮSTATKY, VÝPISY, AVÍZA, ŽÁDOSTI
X	SPOLEČNÉ INFORMACE

Tabulka 4: Kategorie swiftových zpráv

Obsah zprávy je členěn na bloky, kde první blok je povinný pro každou zprávu a další 4 jsou nepovinné dle závislosti na druhu zprávy. Samotná zpráva se skládá ze záhlaví, které v sobě skrývá identifikaci odesílající banky, vstupní pořadové číslo, typ zprávy a ID adresáta swiftové zprávy. Další blok je tzv. textový, ve většině případů nepovinný, má proměnnou délku, maximálně však 95 textových polí seskupených do devíti skupin. Ty nabývají na významu pouze ve vztahu k určité kategorii. Posledním blokem swiftových zpráv je trailer, který je nositel technických informací[48].

Takto vygenerovaná swiftová adresa zvaná BIC[49], je identifikační číslem banky, každá banka má svůj vlastní kód a tím je patřičně oddělena od ostatních, dále BIC obsahuje informace o odesílateli i příjemci v záhlaví swiftové zprávy.

Swiftová adresa je osmi nebo jedenáctimístná, kde jsou na sebe napojeny kódy informující o:

- kód banky (4 abecední znaky)

[48] SWIFT User handbook, září 2003. Dostupné z WWW: http://www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2005/61180/swift_user_handbook_available_online.page

[49] BIC- The Bank Identifier Code, identifikační kód banky.

- kód země (dvoumístný abecední kód např. CZ, DE)
- kód místa (dvoumístný alfanumerický znak regionu či místa uživatele)
- kód pobočky (není povinný, skládá se ze tří alfanumerických znaků)

PŘÍKLADY SWIFTOVÝCH ADRES	
KOMERČNÍ BANKA	**KOMBCZPPXXX**
ČSOB, pobočka Praha 2	**CEKOCZPPR2**
RAIFFEISENBANK	**RZBCCZPPXXX**
HSBC CZECH	**MIDLCZPPXXX**
HSBC USA	**HSBCUS33XXX**

Tabulka 5: Příklady swiftových adres

Kompletní seznam BIC je k nahlédnutí v swiftovém adresáři[50], pravidelně aktualizovaném čtyřikrát ročně.

Do organizace SWIFT může po kladném vyřízení žádosti vstoupit každá banka. Schvalování žádostí podléhá Centrální bance. Po jejím kladném vyřízení je nutno projít zkušebním provozem spočívajícím především v odesíláním a přijímáním testovacích zpráv. V případě splnění těchto požadavků přistupující banka musí zakoupit minimálně jednu akcii, jejíž nominální hodnota činí 5000 belgických franků. SWIFT byla založena jako nezisková společnost, proto poplatky z převodů slouží pouze na náklady provozu celé organizace.

Na závěr můžeme říci, že přechod z dálnopisu na swiftovou síť byl velmi účelný. Přinesl velké výhody především v rychlosti komunikace mezi bankami, v plné automatizaci, zvýšení bezpečnosti a hlavně snížení nákladů na přenos informací.

[50] BIC directory, seznam všech SWIFT kódů, volně přístupný na oficiálních stránkách, volně dostupných na WWW: https://www2.swift.com/directories/

4 Možnosti zneužití elektronického bankovnictví

V současnosti je naše společnost stále více závislá na počítačích a internetových sítích, počet uživatelů intenzivně roste. Rozvoj internetu a bankovnictví změnil chápání nás všech. Není sporu o tom, že ekonomická kriminalita představuje fenomén, jehož rozsah a závažnost v naší společnosti v posledních letech radikálně vzrostly. Důvodem je především proslulá změna ekonomického prostředí, u které není jisté, zda-li se někdy zastaví nebo vrátí do normálu.

Bankovní podvody realizované v oblasti přímého bankovnictví se zaměřením na platební karty a internetové bankovnictví označujeme termínem „bankovní podvody“. Kriminalita bankovních podvodů zahrnuje aspekty trestněprávní, kriminologické i kriminalistické a pohybuje se na pomezí kriminality hospodářské, finanční i informační. Specifické formy protiprávního jednání směřují především k získání přístupových údajů a následném čerpání peněz. V následujících odstavcích bych rád nastínil, do jakých druhů kriminality bankovní podvody patří.

Počítačová kriminalita - Pod tímto termínem můžeme chápat páchání trestné činnosti v níž figuruje počítač jako souhrn technického a programového vybavení včetně dat, případně více počítačů propojených do počítačové sítě. PC může být jak předmětem, tak nástrojem trestné činnosti. A to jak v oblasti ekonomické, sociální i politické. Tento druh postrádá prvky násilí a tím se odlišuje od kriminality klasické. Vzhledem k tomu, že delikty v této oblasti jsou páchány s využitím IT, hovoříme o kriminalitě informační, počítačové nebo kybernetické.

Rada Evropy zavedla pojem Computer Related Crime a definovala počítačovou kriminalitu jako nelegální, nemorální a neoprávněné jednání, zahrnující zneužití dat získaných prostřednictvím informačních a komunikačních medií[51].

Právě počítačová technologie, která by měla ulehčovat člověku práci, se díky svým možnostem stává fenoménem zločinu. Mezi nejznámější a nejvíce diskutované problémy dneška, spojené s počítačovou kriminalitou, patří kriminalita na internetu a softwarové pirátství.

[51] Úmluva o počítačové kriminalitě (Convention on Cybercrime), Budapešť, 23. listopadu 2001.

Finanční kriminalita - je obecně chápána jako součást respektive zvláštní podskupina kriminality hospodářské. Lze ji vymezit jako trestnou činnost páchanou ve finančním sektoru, zaměřenou proti fungování bankovního systému, kapitálového trhu a finančních institucí[52]. Finanční kriminalita převážně spočívá v úmyslné protiprávní činnosti proti majetku, spáchaná v souvislosti s podnikáním finančně investičním a směřující proti němu.

4.1. Pachatel bankovních podvodů

Osoba pachatele bankovních podvodů bývá podle statistik většinou inteligentní vysokoškolsky vzdělaná, zaměřená na technické obory, konkrétně IT. Z hlediska vztahů k informacích je možné pachatele rozdělit na **amatéry**, nezkušené, náhodně hledající zranitelná místa a **profesionály**, nejčastěji organizované skupiny, provádějící soustavnou cílevědomou nelegální činnost za účelem obohacení se. Právě internet se stále více stává nástrojem organizovaného zločinu a do popředí se také dostávají padělky všeho druhu, které bankovní podvody jenom umocňují.

Pachatele především láká vidina snadno vydělaných peněz, dále pak touha po adrenalinu, riziku nebo kompenzace nedostatečného ocenění práce. V dnešní době přetrvávající hospodářské krize a nezaměstnanosti lze očekávat promyšlenější strategie i metody útoku, než které jsme stačili poznat do teď.

Organizovaný zločin - V současnosti organizovaný zločin vnitrostátní, tak i v mezinárodním měřítku využívá často k páchání trestné činnosti prostředků nejmodernější techniky. Trestná činnost páchaná organizovanými skupinami je podle TrZ[53] považována za daleko nebezpečnější, než trestná činnost páchaná jednotlivci.

Specifickou složku tvoří geopolitická situace a rozvoj celosvětových informačních a komunikačních systémů ve státech v postindustriálním stádiu vývoje. Zde vzniká velké nebezpečí zneužití informačních toků mezinárodními zločineckými organizacemi. Z jejich strany hrozí nebezpečí, týkající se

[52] NOVOTNÝ, O. - ZAPLETAL, J. *Kriminologie*. 3. přeprac. vyd. Praha: ASPI, 2008. 355/527 s. ISBN: 978-80-7357-409

[53] Zákon č. 40/2009 Sb., trestní zákoník

poškozování systémů pro místní, národní i světové finanční transakce, burzovní operace, sociální zabezpečení atd.

Podle Útvaru pro odhalování organizovaného zločinu se na podvody s platebními kartami v České republice zaměřují především bulharské gangy[54]. Podle analýzy kriminalistů se u nás od roku 2007 dopouštějí kartových podvodů také organizované skupiny pachatelů rumunské a moldavské národnosti[55], zaměřující se především na padělání platebních karet, které poté používají k výběru finančních obnosů z bankomatů zejména ve východoevropských státech[56]. Organizované zločinecké skupiny jsou často rozděleny do podskupin, jejich struktura často operuje na vybraném území, bez omezení státními hranicemi. Právě světový rozměr se projevuje na nízkém riziku dopadení některého z pachatelů. Vysoký stupeň mezinárodní organizovanosti může např. způsobit, že srbský organizátor může s využitím znalostí čínského informatika řídit krádeže citlivých dat českých občanů. Z těchto dat se padělané karty dají použít kdekoliv na světě, které se rozšíří pomocí dalších osob, kteří z podílů na zisku přebírají hotovost nebo investují do drahých kovů či zboží. Proto dopadení koncového držitele platební karty nevede k rozbití gangu, nýbrž k utržení posledního článku, který je lehce obnovitelný.

4.2 Způsoby bankovních podvodů

Na zneužití platební karty dnes existuje řadou postupů, které se pochopitelně neustále mění a vyvíjí v souvislosti se stále větší vynalézavostí pachatelů trestných činů a jejich technologickou podporou. K zneužití platebních karet napomáhá byť jen nepozornost, neobezřetnost potencionálních obětí a u starších osob především neznalost a důvěryhodnost.

4.2.1 Podvody s platebními kartami

Platební karta je moderní prostředek, který je celosvětově rozšířen. Je využíván k různým způsobům bezhotovostních plateb, výběru hotovosti a dalších finančních transakcí.

---

[54] KOČÍ, P. Virtuální peníze v ohrožení. *Týden*: zpravodajský týdeník, 2008, roč. XV, č. 33, 45 s.
[55] HRADECKÝ, M. – BROŽ, J. Skimming platebních karet v roce 2007. Kriminalistický sborník, 2008, roč. LII, č. 3, 44 s.
[56] Zejména v České republice, Rumunsku, Slovensku a Maďarsku.

Podvody s platebními kartami lze s ohledem na pachatele rozdělit do dvou základních skupin. Mezi první skupinu patří oprávnění držitelé platební karty. Do skupiny druhé pak patří ti neoprávnění. Velmi rozšířené jsou kartové podvody, ke kterým není potřeba mít platební kartu fyzicky při sobě, a to při placení na internetu. Dále bych k těmto podvodům zařadil padělání karet, používání bankomatů, jako prostředků k jejich zneužití a zneužití nedoručené karty.

4.2.1.1 Podvody páchané oprávněnými držiteli karet

Insolvence držitele karty - Nelegální činnost páchaná oprávněným držitelem plat. karty se většinou projevuje ve dvou typech. V prvním případě se jedná o platební neschopnost, tedy insolvenci držitele. Držitel má podvod do předu promyšlen, tedy s úmyslem ho spáchat. Na platební kartě (nejčastěji kreditní), přečerpává zůstatek na účtu a po sléze odmítá dluhy uhradit. Odhalení pachatele zpravidla nečinní potíže, protože v rámci své ochrany si banky vedou databáze, potřebné k vyhodnocování solventnosti ale také kvůli archivaci problémových klientů. To však ale někdy nestačí.

Simulovaná krádež - Druhý druh podvodů lze charakterizovat jako tzv. fiktivní krádež, nebo-li ztrátu platební karty, která je držitelem stanoveným způsobem ohlášena, ale zároveň je používá dále, tím vlastník karty provádí nelegální operace, jejichž výkon připočítává na účet pachatele. Karta se zcela jistě za nějakou dobu zablokuje, proto pachatel má jen omezený čas na tyto neoprávněné úkony.

4.2.1.2 Podvody páchané neoprávněnými držiteli karet

Držitelé platebních karet mohou svou hrubou nedbalostí usnadnit nepoctivému nálezci či zloději, zneužití platební karty tím, že např. u ní mají přiložený PIN kód.

Podstatně kvalifikovanější trestná činnost pochází v úvahu ze strany zlodějů nebo překupníků platebních karet. Ti mají pochopitelně dobré znalosti o aplikačních

možnostech samotné karty, ale i o „obchodních místech“, kde tyto karty mohou konkrétně uplatnit. Mezi nejrozšířenější podvody páchané neoprávněnými držiteli platebních karet patří především:

Horká krádež

Případy tzv. horkých krádeží platebních karet jsou ty, které oprávněný držitel ještě nestačil zaregistrovat. Jestliže v tomto případě má pachatel ještě k dispozici některé osobní doklady držitele, dochází ke značnému odčerpání finančních částek z účtů jejich majitele. Rizikovost při nelegálním výběru vyšších peněžních prostředků nebo finančních transakcí je zvýšena především u speciálních platebních karet tzv. stříbrných, zlatých či diamantových, které se vydávají solventním zákazníkům. Ti mohou při jejich použití přecházet i do značných debetů.

Zneužití osobou blízkou

V úvahu přichází zneužití karet rodinnými příslušníky nebo blízkými osobami, kteří znají PIN kód karty i další nutné individuální údaje. Motivem nemusí být jen majetkový prospěch, ale i rozpad vzájemných vztahů či neshody v rodině.

Krádež a následovné navrácení

Do zmíněné kategorie podvodů patří i forma krádež/navrácení. Název nám říká, že jde o navrácení odcizené platební karty oprávněnému držiteli, který o krádeži nevěděl a ani netušil, že s jeho kartou bylo ilegálně manipulováno a z toho důvodu neučinil kroky k jejímu zablokování. V tomto období dochází k ilegálním výběrům z účtu či pořízení kopii citlivých údajů (tzv. skimming, podrobněji v další podkapitole).

Poškozený se o takto zákeřném zneužití platební karty dovídá často až při měsíčním výpisu účtu a případné reklamace jsou značně problematické.

Zneužití nedoručené karty

Většina peněžních ústavů zasílá platební karty držitelům poštovní cestou, odděleně od zásilky obsahující PIN kód. Protože karta nemá vyplněnou podpisovou kolonku, pachatel má tu možnost kartu podepsat a tak zneužít. Nejbezpečnější formou doručení je v současnosti osobní doručení na přepážce. Platební karta se aktivuje po jejím vyzvednutí a potvrzení PIN kódu oprávněným

držitelem. V opačném případě je karta blokována a nezpůsobilá k provádění transakcí.

4.2.1.3 Zneužití ze strany obchodníků

Upravení prodejních dokladů

Zneužití platebních karet, je možné nejen ze strany držitelů karty (oprávněných, neoprávněných), ale i z pozice třetí strany jakou je samotný obchodník. Jedná se o tzv. přepsané prodejní doklady. Tento způsob lze uskutečnit pouze s embosovanými platebními kartami, jejichž informace jsou snímány zařízením zvaným imprinter. Ten vytváří kopie platebních karet na papírový předtisk a zároveň v něm uvádí ID daného obchodního místa. Vyhotovuje ve třech kopiích pokladní doklad, který je po autorizaci podpisu předán kupujícímu, druhý si ponechá obchodník a třetí je zaslán zúčtovací bance. Obchodník může ilegálně upravit inkasovanou částku na svém dokladu i na dokladu, který posílá k zúčtování. Pokud si vlastník karty neuchová kopie dokladu, tak se v případě reklamace dostává do důkazní nouze.

Vícenásobné transakce

Bohužel z pozice obchodníků přicházejí v úvahu i další ilegální podvody s platebními kartami. Např. vícenásobné kopie, při kterých obchodník opakovaně vystaví bianco otisk platební karty, aniž by o tom držitel věděl, který po sléze opatří padělaným podpisem. Tento trik vlastník platební karty obchodníkovi umožní tím, že ji ztratí ze svého dohledu, např. tím, že ji předá číšníkovi. Prevence tohoto podvodu je zřejmá, nenechávat platební kartu bez Vaší fyzické kontroly.

4.3 Padělání karet

Podobná jednání spojená s paděláním platebních karet vedou k obrovským finančním ztrátám, jak ze strany klientů, tak i emitentů. Platební karty jsou v dnešní době jeden z nejběžnějších způsobu platby za zboží a služby. Vždyť počet platebních karet vydaných v ČR již přesahuje 4,6 mil., a počet obchodních míst, které platební karty akceptují již přesahuje 38 tis. Ročně je těmito kartami

v ČR provedeno více než 130 mil. transakcí, přičemž objem peněžních prostředků při těchto transakcích přesahuje 295 mld. korun[57], proto je tento obor takovým lákadlem pro organizovaný zločin. Ztráty se sčítají průměrně ve stovkách miliónů EUR ročně, i když se publikované údaje zřejmě neshodují s realitou, protože mnoho poškozených z různých důvodů nemá zájem o publikaci reálné výše ztrát.

V ČR již existují zkušenosti s vyšetřováním a postihováním tohoto jednání, ale ne vždy orgány činné v trestním řízení dokážou tento skutek správně právně kvalifikovat. Výše popsané jednání se dá kvalifikovat a trestně stíhat jako tr. čin padělání a pozměňování peněz dle § 140 tr. zákona s odkazem na § 143 tr. zákona, neboť platební karta požívá ochrany též jako bezhotovostní platební prostředek[58].

4.3.1 Pozměňování ochranných prvků karet

Padělání karet spočívá ve vyhlazení či deformaci původních informací z karty za pomocí tepelné úpravy a poté vytlačení údajů nových. Lze je provádět jen u embosovaných platebních karet. U tohoto mechanického způsobu dochází většinou k barevným změnám na povrchu karty, které jsou velmi snadno odhalitelné. Kvůli těmto způsobům platební karty obsahují ochranné prvky, jako je např. hologram, ceninový tisk či podpisový proužek. Dnes jsou karty vyráběny také ze speciálních polykarbonátů, citlivých na nejrůznější chemikálie či gumování.

4.3.2 Skimming

Další z velmi rozšířených druhů páchání trestné činnosti, který vede k padělku platební karty je bezesporu tzv. skimming. Tímto termínem bývá označován způsob páchání trestné činnosti, při které dochází k nedovolenému zkopírování údajů z magnetického proužku bez vědomí oprávněného držitele platební karty. Je

[57] VICHEREK, Roman. Padělání a pozměňování platebních karet z trestněprávního hlediska. *Www.justic.cz* [online]. [cit. 27.2.2012] Dostupné z: http://trestni.juristic.cz/524757/clanek/trest3.html

[58] Tamtéž

považován za nejnebezpečnější a nejzávažnější formu[59]. Přesněji tento způsob spočívá v přípravě či výrobě různých zařízení, které jsou pachateli nasazovány na nejrůznější předměty, jako jsou: bankomaty, imprintery, zkrátka všude tam, kde se dá použít platební karta. Pachatel v první fázi nejprve nelegálně zkopíruje data z magnetického proužku nebo čipu. K tomu se využívají miniaturní zařízení, které je možno skrýt třeba v dlani a pachatel může odčerpávat informace z karty třeba při komunikaci s Vámi. Mám na mysli např. číšníka, kterému zrovna předáváte kartu k zaplacení útraty v restauraci. Často se také zařízení aplikují na čtečku karet u vstupních dveří k bankomatům. Tyto nashromážděná data jsou ukládána buď ve skimmovacím zařízení nebo rovnou odesílána pomocí bezdrátového přenosu dat do mobilu či počítače. V průměru kapacita skimmovacích zařízení pojme 200 záznamů dat z platebních karet. Další fáze skimmingu spočívá ve vytvoření klonu karty na vytvořenou bianco kartu.

Obr. 5: Skimmovací zařízení

Obr. 6: Bankomat, šipky znázorňují skimmovací zařízení

Obrázek 7: Příklad skimmovací klávesnice

[59] SADOVSKÝ, D. – SUCHÁNEK, J. Platební karty a možnosti jejich zneužití. *Kriminalistika*: časopis pro kriminalistickou teorii a praxi, 2004, roč. XXXVII, č. 1, s. 26.

Pachatel buď kartu vyrobí kartu novou nebo použije již existující, např. věrnostní, neplatnou bankovní či telefonní kartu, z které informace předtím vymazal. Důležité je, aby karta obsahovala magnetický proužek nebo čip.

K dokonalosti skimmingu chybí znalost kódu PIN. V mnoha případech pachatelé sledují držitele karty při zadávání PIN kódu na klávesnici bankomatu. Vynalézavost organizovaných skupin v tomto odvětví je opravdu vysoká a rozmanitá. Používají kromě fyzického sledování, také mnohem technologicky promyšlenější způsoby, jak bezchybně pomocí prstů držitele účtu zjistit přístupový kód. A to instalací miniaturních kamer, či falešných klávesnic, které rovnou snímají a přeposílají PIN do počítače pachatele. Po této složité operaci, je padělaná karta připravena k výběru hotovosti či platbě za zboží a tváří se jako karta pravá. Výsledkem skimmingu je tedy nezákonné čerpání peněžních prostředků.

4.4 Internetové podvody

Lze je chápat jako kartové podvody bez fyzické přítomnosti platební karty. V principu se jedná o zneužití podvodně získaných údajů z platebních karet, které se využívají především k nákupu prostřednictví telekomunikačních prostředků (internetové, telefonní či písemné objednávky). V ČR se tento typ naštěstí moc nerozšířil, ale za hranicemi je to jeden nejčastějších způsobů zneužití elektronického bankovnictví.

Odcizené údaje platebních karet se objevují k prodeji na internetových stránkách (např. dumps.co.nr. cc-info.biz nebo cvv-sell.com)[60]. V roce 2006 byla prodejní cena jednoho čísla platební karty se jménem majitele, datem expirace a CVV/CVC kódem asi 100 amerických dolarů[61]. Dnešní prodejní cena údajů platební karty je asi desetkrát až dvacetkrát nižší. Tržní cena údajů evropské platební karty začíná na 5 USD. Údaje z amerických platebních karet jsou k prodeji dokonce o 1 USD méně. Zní to až nemožně, ale někteří prodejci bankovních dat nabízejí i záruku platnosti prodávaných údajů.

[60] KOČÍ, P. Virtuální peníze v ohrožení. *Týden*: zpravodajský týdeník, 2008, roč. XV, č. 33, s. 46.
[61] KOČÍ, P. Virtuální peníze v ohrožení. *Týden*: zpravodajský týdeník, 2008, roč. XV, č. 33, s. 47.

4.4.1 Phishing

Tento druh internetového podvodu je někdy do češtiny překládán jako „rybaření“. Možná Vám připadá, že rybaření se anglicky píše jinak, ale tento podvod nedostal překlad doslovný, nýbrž podle způsobu páchání, který se opravdu rovná nahození návnady a čekání na úlovek. Podstatou phishingu je získání citlivých dat (hesla, PIN, čísla karet) prostřednictvím rozesílaných emailových zpráv, které se tváří jako by Vás kontaktovala Vaše banka.

V emailu jste vyzváni k zadání citlivých údajů, pokud tomuto útoku podlehnete, Vaše karta bude během několika minut zneužita pomocí transakcí prováděné na internetu. V zájmu klienta a prevence je ideální na takové zprávy vůbec nereagovat a uvědomit si, že banka nikdy takové data přes internet nebude vyžadovat.

Velmi často se tyto emailové útoky vyznačují kostrbatou češtinou a gramatickými chybami, je to dáno doslovným elektronickým překladačem typu google translator[62], protože pachatelé ve většině případů nejsou Češi.

4.4.2 Pharming

Někdy překládáno do češtiny jako „farmaření“. Je druh internetového podvodu, jehož princip spočívá v napadení DNS[63] a přepsání IP adresy. Má za úkol přesvědčit uživatele, že se přihlásil do internetového bankovnictví své banky, ale přitom se nalogoval do přesměrovaných stránek podvodníků. Na základě zadaných údajů může dojít k odcizení peněz z účtu. U tohoto podvodu je nutné věnovat pozornost vzhledu přihlašovací stránky. Banky vždy využívají SSL protokol[64].

---

[62] Překladač Google překládá zdarma a rychle z 58 různých jazyků. Dokáže přeložit slova, věty a webové stránky v libovolné kombinaci podporovaných jazyků.

[63] DNS (z angl. Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Slouží k překladu slovních adres.

[64] Secure Sockets Layer, SSL (doslova *vrstva bezpečných socketů*) je protokol, resp. vrstva vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP, která poskytuje zabezpečení komunikace šifrováním a autentizací komunikujících stran.

5 Nebankovní elektronické platební systémy

Vývoj a rozšíření elektronických platebních systémů jde díky technologickému vývoji stále dopředu a s ním i poptávka veřejnosti. Elektronizace umožňující dálkový přístup k účtu, ať už k bankovnímu či nebankovnímu je stále vyspělejší a v mnoha ohledech také levnější a bezpečnější.

Nebankovní elektronické systémy jsou mechanismy, které poskytují nástroj pro převod peněz mezi subjekty, nedochází zde k vzniku či zániku, ale pouze k změně vlastníka finančních prostředků. Pojem nebankovní je na první pohled zřejmý, společnosti poskytující platební systémy, nemusejí být podle české právní úpravy akciové společnosti se sídlem v ČR, nemusejí přijímat vklady a poskytovat úvěry veřejnosti a hlavně nemusí disponovat bankovní licencí. Zákon tedy říká, co je banka, pak je tedy jednoduché vymezit pojem nebankovního subjektu. Jsou to osoby na které se nevztahují právní úpravy určené bankám, nepodléhají bankovnímu dozoru a nejsou nositeli bankovní licence. To však neznamená, že nevykonávají některé služby, které jsou pro bankovní instituce typické. O bankovních platebních systémech jsem hovořil v minulých kapitolách. VISA, MasterCard, American Express a jiné jsou sice nebankovní společnosti, avšak do bankovních platebních systémů je řadíme proto, že zprostředkovávají převod peněžních prostředků z jednoho bankovního účtu na druhý a v podstatě představují jen jiný druh přístupu k bankovním prostředkům. Dnes již máme k dispozici nespočet nebankovních společností nabízející služby tohoto typu, rozhodl jsem se podrobněji popsat největší z nich a to PayPal.

5.1 Přednosti elektronického platebního systému

K tomu, aby byl platební systém konkurenceschopný, musí splňovat mnoho požadavků, které od něj klienti očekávají.

Pevně věřím, že doby, kdy na internetu fungovalo vše jen z části jsou už pryč. Ať to byly důvody nedokonalého připojení, chybného naprogramování webové stránky nebo aplikací. K tomu aby byl jakýkoliv produkt bonitní, musí být především spolehlivý a dostupný.

Mezi přednosti elektronických platebních systémů patří především možnost vstupu odkudkoliv, kde je pokrytí internetové sítě. Tyto výhody jsou v celku shodné s internetovým bankovnictvím popsaným výše.

První rozdíl, který najdeme mezi bankovními a nebankovními systémy je ve spolehlivosti. Bankovní systémy jsou mnohem lépe jištěny a proto celkový výpadek sítě je zcela výjimečný, oproti tomu u nebankovních společností poskytujících elektronické platební systémy se to čas od času stane.

Velmi důležitým aspektem platebních systémů při poskytování platebních služeb je především jeho práce s osobními údaji. Klienti na utajení těchto informací kladou stále větší důraz a očekávají, že se tyto informace dozvědí pouze oni a platební společnost, která je v rámci zákona a konkurenceschopnosti povinna s nimi nakládat tak, aby je nikdy nikdo nezneužil.

Další rozdíl mezi bankovními a nebankovními systémy je v rychlosti přesunu peněz z jedno účtu na druhý. Banky často mají tendenci peníze pozdržovat, důvod je jasný. Od odeslání peněz do přijetí běží uměle vytvořená lhůta, při které banka dostává peníze „zadarmo“ a může je úročit u centrálních bank. Většinou převody mezi bankami trvají i několik dní. Na druhé straně u nebankovních společností tato potřeba chybí a odeslání i připsání peněz je takřka okamžité. Dá se tedy říci, že některým požadavkům vyhovují více bankovní systémy a některým systémy nebankovní. Koneckonců záleží na koncovém zákazníkovi, jaké si zvolí priority a jaká společnost mu bude nejvíce vyhovující.

5.2 PayPal

PayPal je jedním z nejznámějších a zároveň z nejrozšířenějších elektronických nebankovních platebních systémů.

Právě v roce 1998 poprvé Kalifornská společnost Confinity, se sídlem v Sillicon Valley představila svůj první internetový systém ze svého obrovského IT repertoáru. Většinu firem operujících ve stejné branži postihl po velkém rozkvětu ještě větší pád. PayPal se i navzdory problémům na počátku svého vývoje a krizi, která firmu postihla drží na vrcholu ve své kategorii do dnes. Jako mnoho úspěšných programů či produktů ani PayPal nevznikl prvotně k účelu, jak ho známe dnes, tedy k převodu finančních prostředků při nákupu na internetu. Prvním konkrétním účelem bylo zprostředkování převodu peněz při nákupu

aplikací a knih pro společnost Palm, která se proslavila především svými PDA a MDA přístroji, které svou funkcí a vzhledem inspirovaly dnes velmi moderní tzv. chytré telefony. PayPal u Palmu dlouho nevydržel a nahradil svou platformu na zcela internetové rozhraní.

Svého vrcholu, co se týče rozvoje dosáhl v roce 2000, kdy každý den rostl počet jeho uživatelů o 10% po dobu tří měsíců. Značnou zásluhu na tento boom má zcela jistě masivní kampaň, která v roce millenia PayPal doprovázela. Společnost poskytovala bonus 10 USD každé osobě, která si založila nový účet. Lidé se snažili systém obejít všemi možnými způsoby, tím že si zakládali více účtů pomocí počítačových automatických robotů a inkasovali bonusový poplatek hned několik tisíckrát. Značná expanze, ale také podvody spojené s registrací překvapily samotnou společnost a ta se dostala do ztráty. Ve své největší krizi PayPal prodělával 10 mil. USD za měsíc.

Aby toho nebylo málo, celosvětová aukční síň Ebay oznámila spuštění svého vlastního platebního systému Billpoint, který se stal přímým konkurentem firmy ze Sillicon Valley. Právě Ebay.com bylo největším konkurenčním prostředím pro obě společnosti, kde si PayPal i přes takřka bojové prostředí udržel značnou popularitu. Ebay prosazoval Billpoint jako oficiální platební systém svého aukčního portálu a tím zúžil pole působnosti pouze pro jeden internetový server. Tento krok nahrál do karet „modrobílé konkurenci“[65]. Největší aukční síň na světě se situaci rozhodla řešit po svém a to snahou omezit platební systém pouze na Billpoint. Tomuto tlaku se společnost Confinity ubránila za pomocí pravidel na ochranu hospodářské soutěže. Velmi sledovaný konkurenční boj skončil poměrně překvapivým, ale logických výsledkem. V říjnu 2002 Ebay oznámil koupi PayPal, jeho tehdejší platební systém Billpoint přestal existovat a tím přestala existovat i v té době jediná konkurence schopná „virtuální peněženka“. Tím se PayPal dostal na vrchol ve své branži, kde se nachází dodnes. Tento internetový platební systém užívá přes 100 mil. uživatelů na celém světě.

[65] Logo systému PayPal se skládá z modrého názvu na bílém poli.

5.2.1 Registrace a funkce

Registrace do rozhraní Paypal je založena především na jednoduchosti. Pro úspěšnou aktivaci účtu je potřeba mít pouze vlastní emailovou adresu a platební kartu. Na počátku procesu si vyberete typ účtu, PayPal nabízí trojici rozdílných účtů a to: Personal account, Premier account a Business account[66]. Po vybraném účtu si zvolíte stát, ze kterého pocházíte, vyplníte dvě kontrolní otázky a potvrdíte obchodní podmínky. Po vyplnění základního formuláře Vás PayPal vyzve k poskytnutí informací z platební karty, akceptuje tyto: VISA, MasterCard, VISA Electron a American Express.

Systém pro ověření totožnosti je vymyšlen velmi důmyslně. po aktivaci karty se z ní odečte 1,5 EUR a připíše se na PayPal účet. Ve výpisu transakcí na Vaší bankovní kartě se objeví čtyřmístný kód, který vložíte na PayPalu a aktivace Vašeho internetového účtu je připravena k použití.

Prostřednictvím PayPalu je možné platit na všech serverech s jeho podporou. Jak jsem již napsal, největší využití představuje na internetové aukční síti eBay a nyní i na telekomunikačním serveru Skype. Na svůj účet u PayPal převedete peníze ze své platební karty, platit však lze i bez „dobití". Pokud zde není dostatek peněz je provedeno inkaso z platební karty, kterou máte k účtu zaregistrovanou. Výhodou tohoto postupu je především to, že číslo vaší karty a ani jiné informace se vůbec neposkytují obchodníkovi, jemuž platíte[67].

PayPal je systém umožňující pohodlně a bezpečně odesílat a přijímat internetové platby. Působí v 55 zemích světa a jen v Evropě ho využívá přes 160 tisíc internetových obchodníků. Ne všechny ale mohou využívat všechny jeho služby, ale pouze tzv. send only service, které znamenají, že takto přijaté peníze nelze převést na klasický bankovní účet. PayPal tímto vstupuje do boje proti nepoctivým obchodníkům ze všech koutů světa a zamezuje tím praní špinavých peněz. Tímto omezením sice ubírá na kvalitě služeb, ale na druhou stranu posiluje věrohodnost serveru a tím naši bezpečnost. Pro některé uživatele se tak PayPal doslova stává jen „poloplatebním" systémem[68].

---

[66] Typy účtů u PayPal se liší především v počtu funkcí, poplatku za zřízení a především výší provize za přijatou platbu.

[67] RUML, M. PayPal konkuruje našim bankám. ***Www.finance.cz*** [online]. 2006 [cit. 14.3.2012]. Dostupné z: http://www.finance.cz/zpravy/finance/80569-paypal-konkuruje-nasim-bankam/

[68] Www.paypal-dobijeni.cz: [online]. Dostupné z WWW: https://www.paypal-dobijeni.cz/co-je-paypal.php

Od června roku 2006 byl PayPal přístupný i pro občany ČR, a to ve výše zmíněné omezené formě - pouze pro posílání peněz a placení kartou. Od září 2010 však začal PayPal ve svém platebním systému podporovat i účty v českých korunách a platby prostřednictvím PayPal je možné nejen odesílat, ale i přijímat. Češi mají nově i možnost většího výběru měn, v nichž je jejich PayPal účet veden. Zatímco doposud bylo možno vybírat ze šesti měn, nyní jich mají k dispozici 16, přičemž uživatel může mít otevřeno všech 16 účtů najednou. Dosud byl tedy u nás PayPal využíván nejvíce jako prostředek pro platby na internetu a pro posílání menších částek do zahraničí. Nyní však může PayPal využít i ten, na jehož účet prostředky přicházejí. Pro něj už ale PayPal tak výhodný jako pro odesílatele platby být ani zdaleka nemusí, protože jak jsme již zmínili výše, poplatky za platbu nese příjemce platby. Poplatek je ve výši určitého procenta (kolem 3%, podle obratu) z výše přijaté platby plus určitý poplatek (10 Kč) za každou platbu. Takže logicky, čím vyšší platbu posíláte, tím vyšší poplatek zaplatíte. Naopak u drobných plateb je výše poplatku zanedbatelná. Jedná-li se však o převod mezi dvěma účty stejné měny a pokud není realizován prostřednictvím platební karty, je i příjem peněz zdarma.[69]

5.2.2 Zabezpečení

Po pirátských útocích při zrodu společnosti, které se snažili vydělat na dotacích spojených se zakládáním účtů počítačovými roboty, se PayPal musel rychle vzpamatovat a způsob řešení tohoto problému vyústil v další revoluci z rodiny PayPal a to vytvořením systémem CAPTCHA[70], který nutí každého nového uživatele k ručnímu přepsání různě zohýbaného textu, který je pro roboty nečitelný. PayPal do tohoto systému vložil nemalé peníze a sám sebe považuje za tvůrce, ovšem existují důkazy, které dokládají existenci Turingova testu ještě před PayPalem. Jedno se dá říci ale jistě, PayPal byl první, kdo sytém CAPTCHA masivně rozšířil po celém světě.

Hlavní výhodou platebního sytému PayPal je velmi šetrné použití platební karty, jejíž informace sdělíte pouze společnosti, nikoliv pak tomu, kdo platbu

[69] RUML, M. PayPal konkuruje našim bankám. *Www.finance.cz* [online]. 2006 [cit. 14.3.2012]. Dostupné z: http://www.finance.cz/zpravy/finance/80569-paypal-konkuruje-nasim-bankam/

[70] CAPTCHA je Turingův test, který slouží k rozlišení lidí od robotů kvůli kybernetickým podvodům.

přijímá. Prodávající uvidí pouze Váš email, pomocí kterého platbu identifikuje během několika sekund po odeslání peněz. Tím se eliminuje riziko, aby si nárokoval větší platbu než mu přísluší.

Obr. 8. Příklad systému CAPTCHA[71]

Díky svému gigantickému rozšíření je u PayPalu dost pravděpodobné, že bude mít více negativních ohlasů, než ostatní servery tohoto typu. Mezi značné nevýhody patří především absence multi-level marketingu, totiž neexistují zvýhodněné programy pro velké korporace, které disponují s mnohem větším obratem a tím pádem většími provizemi pro PayPal. Další vlastností, která se pyšní značnou negací je existence výše zmíněný „send only service“, tedy možnost pouze odesílání peněz bez přijetí. Na druhou stranu tyto body kritiky jsou součástí systému a je na vůli majitele, jaké si zvolí obchodní podmínky. Ty ale nejsou zrovna pro uživatele přívětivé, už jen, že mají rozsah 35 stran textu, obsahují problematická ustanovení, které se velmi často mění. Navíc podobných ustanovení je v kompletních obchodních podmínkách velké množství a umožňuje tak společnosti odstavit účet libovolně při jakékoliv transakci. V případě podezření je společnost PayPal vyšetřovatelem, soudcem, porotou i vykonavatelem zároveň, a to bez možnosti jakéhokoliv odvolání. Dá se tak říci, že při používání PayPal vydává uživatel svoje finance na pospas libovůle provozovatele. Pokud přece jen společnost uzná svoji chybu podle svých obchodních podmínek, klient může čekat až 180 dní na vrácení peněz. Na uživateli zůstává volba přizpůsobit se či PayPal nepoužívat. Kritika však dorostla do takové míry, že vznikla webová stránka www.paypalsucks.com, která se zabývá negativními ohlasy s používáním PayPalu. Ta se díky své návštěvnosti

[71] Zdroj: http://cmp.felk.cvut.cz/~hadacja2/experiments/report_2/google.png

probojovala až do „Top ten corporate hate websites“, kterou pravidelně sestavuje prestižní časopis FORBES[72].

Měsíční prodej přes PayPal	Cena
0 - 70 000,-	3,4% + 10,-
70 001 - 280 000,-	2,9% + 10,-
280 001 - 1 500 000,-	2,7% + 10,-
1 500 001 - 3 000 000,-	2,4% + 10,-
>3 000 000,-	1,9% + 10,-

Tabulka 6:Přehled poplatků v síti PayPal[73]

PayPal ale není založen pouze na negativních ohlasech, to by nebyl, tam kde je dnes. Mezi jeho největší priority vedle rychlého a bezpečného převodu peněz patří produkt „ochrana zboží PayPal“, prostřednictvím tohoto patentu, poskytovatel ručí za veškeré hmotné zboží, které může být doručeno prostřednictvím pošty. Tedy když zaplatíte nepoctivému prodejci a ten Vám pošle buď vadné zboží nebo ho nepošle vůbec, tak PayPal odpovídá za náhradu škody a to je na poli internetových aukčních sítí ta největší výhoda, kterou Vám může poskytovatel platebního styku poskytnout.

5.3 Jiné platební systémy

Mezi další elektronické nebankovní platební systémy typu PayPal poskytující své služby na území ČR, můžeme zařadit: PayPay, PayMyway, Paysafecard a PaySec. Jak je vidět, seznam společností začínající výrazem „PAY“ a provozující „virtuální peněženky“ je opravdu nepřehledný. Jsou to v podstatě systémy založené na podobném obsahu, které se liší opravdu jen v detailech, jako jsou poplatky, způsobem dobití finančních prostředků, různorodosti měny. V podstatě, jakou společnost si zvolíme do značné míry ovlivňuje samotný internetový

[72] Forbes - soukromá vydavatelská mediální společnost, která existuje od roku 1917. Sídlí v New Yorku na 5th avenue. Proslavila se především pravidelnými žebříčky nejbohatších lidí planety.
[73] Www.paypal.cz: poplatky za platby. [online]. Dostupné z: http://www.paypalcz.cz/poplatky-za-platby

obchod, protože bez jeho podpory daného platebního systému ho použít nemůžeme. Jaká platební společnost je podporována na daném eshopu zjistíme většinou hned na hlavní stránce, kde se chlubí jejich logem, pokud ne jistou odpověď se dozvíme z obchodních podmínek.

PaySec

Je v podstatě mladý poskytovatel, na trhu poskytuje své služby přes 4 roky. Je výtvorem ČSOB a České spořitelny. Mezi jeho výhody patří především možnost platby ve více než 500 eshopech v ČR, snadné dobíjení pomocí bankovního účtu či platební karty. Mezi značné nevýhody bych zařadil poplatky za dobíjení konta platební kartou a nemožnost dražších nákupů (nad 100 tis.).

PayPay

Je velmi podobný svému konkurentovi PayPal. Peníze na PayPay vám může poslat i člověk, který tuto službu nevyužívá. Důležité je, aby znal specifický symbol vašeho účtu na PayPay. Otevření, vedení účtu a posílání peněz v rámci PayPay je zdarma. Výběr peněz a zaslání na ověřený bankovní účet stojí 20 korun. Přijetí peněz z účtu je zdarma, ale z platební karty zaplatíte pět procent z částky plus deset korun. Ve shrnutí mezi klady patří možnost vedení účtu v cizích měnách a je levnější než PayPal. Mezi zápory patří, že si účtují poplatek za příjem peněz z platební karty.

Paysafecard

Společnost založena na trochu odlišné bázi, než společnosti zmíněné výše. Společným bodem je tedy to, že slouží pro platby na internetu bez přímého použití platební karty. Paysafecard je doslova předplacený kredit pro nákup na internetu, prodává se na svých prodejních místech (benzínové stanice, trafiky atd.) jako karta s nabitou částkou 100, 200, 500, 1000 nebo 2000 Kč. Na účtence je vygenerován 16 místný PIN, který vložíte při platbě na stránkách s jeho podporou a máte zboží zaplaceno. Velké pozitivum přisuzuji možnosti dobití 100 korunových částek, to je vhodné především pro studenty a dále veliké množství dobíjecích míst. Mezi negativa bych zařadil: nemožnost vysokých plateb, kredit nelze nabít z domova přes běžný účet a také nepříliš velká podpora internetových obchodů.

PayMyway

Nejmladší z těchto čtyř „virtuálních peněženek“. PayMyway je novinkou spočívající také na odlišném způsobu provedení platby. Jde o propojení internetového bankovnictví a samotného obchodu, aniž by prodávající viděl Vaše bankovní informace. U internetových obchodů, které tento způsob platby podporují, Vy zadáte platbu pomocí PayMyway, systém vygeneruje předvyplněný platební příkaz, Vy ho potvrdíte prostřednictvím internetového bankovnictví a obchodník dostane informaci o autorizované platbě. Jak už jsem řekl, tento systém je mladý a zatím ho podporuje pouze jeden internetový obchod a to www.123shop.cz.

6 Právní úprava bankovnictví

Každý z nás se neustále pohybuje ve složité síti vzájemně provázaných společenských vztahů, jejichž obsah a význam je definován mnoha faktory. Nejvýznamnější faktor je právní řád, který dává každému právnímu vztahu jeho definici a tím i jeho obsah a význam. Všechny instituty, ať už sociologické, ekonomické či vědecké je možno zkoumat z právního hlediska a právě problematika bank, elektronických peněz, platebních systémů a elektronického bankovnictví není výjimkou.

Bankovnictví je obor, na jehož bezchybné fungování je společností i zákonodárci kladena mnohem větší pozornost, než u jiných odvětví. Proto se v následující kapitole budu věnovat právní úpravě tohoto fenoménu, konkrétně základnímu zákonu o bankách, udělování bankovních licencí, právní regulaci platebního styku, problematice elektronických peněz, dozoru nad bankami a v neposlední řadě také České národní bance. Pokusím se detailněji představit právní úpravu nám nejbližší, tedy úpravu v České republice s odkazem na primární a sekundární právo Evropské unie, které je aplikačně nadřazené našemu právnímu řádu.

Bankovnictví jako celek je upraveno celou řadou právních předpisů. Proto bych se rád v této kapitole zaměřil na významné právní úpravy tohoto odvětví.

Již náš nejvyšší zákon Ústava ČR zakotvuje v čl. 98 existenci ČNB, jako centrální banky. Obchodní banky a jejich služby jsou významnou součástí finančního trhu, jsou ekonomicky napojené na nemalé množství subjektů (právnických i fyzických osob) a jejichž existence je na nich více než závislá. Ať už se jedná o úvěry či správu peněz je potřeba tyto finance chránit před nepříznivými vlivy.

Nejdůležitější právní úpravou v oblasti obchodních bank je rozhodně zákon č. 21/1992 Sb., o bankách a zákon č. 284/2009 Sb., o platebním styku. Ukládají základní ustanovení v oblasti samotné existence bank, udělování licencí, dohledu nad bankami a jejich zánikem. Po vstupu ČR do EU se pro nás staly právně závazné směrnice a nařízení vydané orgány Evropské unie. Ačkoliv sekundární právo EU je pramenem práva, právní předpisy a jejich novelizace jsou vydávány tak, aby byly v jisté harmonizaci s normami Evropské unie.

Nejvýznamnější směrnice EU v oblasti elektronického bankovnictví po novele zákona č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb., jsou:

- Směrnice Evropského parlamentu a Rady 2007/64/ES o platebních službách na vnitřním trhu, která změnila směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES, ve znění směrnice Evropského parlamentu a Rady 2009/111/ES.

- Směrnice Evropského parlamentu a Rady 2009/44/ES, kterou se mění směrnice 98/26/ES o neodvolatelnosti zúčtování v platebních systémech a v systémech vypořádání obchodů s cennými papíry a směrnice 2002/47/ES o dohodách o finančním zajištění, pokud jde o propojené systémy a pohledávky z úvěru.

- Směrnice Evropského parlamentu a Rady 2009/110/ES o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností, která nahradila směrnici 2005/60/ES a 2006/48/ES a o zrušila směrnici 2000/46/ES.

Banky v České republice mohou být pouze právnické osoby, založené jako akciové společnosti. Bankovní instituce mají svůj jednotlivý charakter, kterým se mezi sebou liší, rozdělujeme je na univerzální a specializované. Rozdíl mezi nimi je především v míře povolených činností. Specializované banky jsou zaměřeny jen na určité segmenty, mají povolení působit jako banka pouze v rámci konkrétní činnosti. Banky univerzální mají povolení působit ve všech nebo ve většině bankovních činnostech.

6.1 Bankovní licence

Banky, aby mohly provozovat svou podnikatelskou činnost, jako je např. přijímání vkladů, poskytování úvěrů, investování do cenných papírů, platební

styk, vydávání a správa platebních prostředků, směnárenská činnost[74] atd. musejí vlastnit bankovní licenci, s níž se pojí výkon pouze těch činnosti, které jsou v licenci povolené.

O vydání této licence rozhoduje na žádost Česká národní banka, ke které vydává stanovisko orgán dohledu členského státu EU. Podmínek pro vydání licence je opravdu mnoho a je z nich zřejmé, že podnikání v bankovnictví není vhodné pro každého a vyžaduje vysokou dávku odbornosti, profesionality a kapitálu.

Minimální výše základního kapitálu musí činit 500 000 000 Kč, který musí být splacen v celé výši a dále zákon vyžaduje, aby byl doložen jeho nezávadný původ. Vysoké nároky jsou kladeny také na nejvyšší vedení samotné banky a to především na důvěryhodnost a odbornou způsobilost osob ve výkonných řídicích funkcích a osob s úzkým propojením s bankou. Velmi důležitý je i čistý trestní rejstřík těchto osob. Česká národní banka dále vyžaduje dokonalý obchodní plán, strategii a reálnou ekonomickou rozvahu[75]. Sídlo budoucí banky musí být na území České republiky, to se však netýká zahraničních bank, které se chystají otevřít pobočku na našem území. Žádost o licenci zahraničních bank má v podstatě stejné požadavky, jako u bank domácích. Nemůže například provozovat činnosti v hostitelském státě, které neprovozuje ve státě domovském a před založení pobočky má povinnost kontaktovat orgán dohledu domovského státu a sdělit mu informace potřebné k posouzení správné organizační struktury a finanční situaci banky. V případě žádných nedostatků, domácí orgán dohledu předá tyto informace do 3 měsíců hostitelskému orgánu dohledu, který se připraví na dohled nad finanční institucí. Po uplynutí 2 měsíců může banka na území hostitelského státu začít podnikat[76].

Nad dodržováním předpisů u poboček bank cizích států dohlíží kontrolní orgán hostitelského státu. Pokud zjistí porušení právních předpisů, které spadají do jeho působnosti, nejdříve požádá banku o ukončení protiprávního stavu. Pokud banka tak neučiní, tento orgán může požádat domovský orgán dohledu banky k přijetí potřebných opatření. Jestli i tyto úkony nevedou k nápravě protiprávního stavu, kontrolní orgány mohou ukončit činnost banky odnětím licence. To však není jediný způsob zániku licence, dalšími jsou: zrušení banky s likvidací nebo výmazu banky z obchodního rejstříku. Dále cizí bance, která provozuje pobočku v České

[74] §1 odst. 2, 3, Zákon č. 21/1992 Sb., o bankách
[75] §4 odst. 3,4,5,6,7, Zákon č. 21/1992 Sb., o bankách
[76] §5g, §5h, Zákon č. 21/1992 Sb., o bankách.

republice zaniká licence ukončením svého působení na tomto území nebo pokud pozbyla oprávnění ve státě svého sídla[77]

6.2 Zákon o České národní bance

Českým orgánem vykonávajícím kontrolu nad bankami je Česká národní banka. Zvláštním českým právním předpisem, který upravuje postavení ČNB, je zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů, který byl 3. ledna 2012 předložen Ministerstvem financí po dohodě s ČNB. Cílem návrhu bylo odstranit některé nekompatibility platného zákona s právem Evropské unie, které byly opakovaně kritizovány v konvergenčních zprávách Evropské komise a Evropské centrální banky. Návrhem současně dochází ke zrušení Výboru pro finanční trh a institutu opatření České národní banky, k podrobnější právní úpravě výkaznictví a statistiky a k nápravě některých aplikačních nedostatků a nejasností stávajícího znění zákona[78].

Dohled spočívá v omezení rizika, která jsou spojena s činností bank. Jde především o rizika obezřetného podnikání a bezpečném fungování bankovního systému. Bankovní dohled zahrnuje: posuzování žádosti o udělení povolení působit jako banka, dohled nad stanovenými podmínkami, právními předpisy a opatření vydaných ČNB a v neposlední řadě ČNB může ukládat opatření k nápravě a to udělením pokut nebo příkazem upustit od nesprávného postupu či ukončení činnosti. Všechny osoby, které dohled tohoto typu vykonávají mají povinnost mlčenlivosti o všech informacích, které se dozvěděly v souvislosti s výkonem svého povolání, která trvá i po skončení této funkce[79]. Kontrolní činnost mezi ČNB a bankou se řídí základními pravidly kontrolní činnosti podle z.č. 52/1991 Sb., o státní kontrole.

Kromě výše uvedených činností, ČNB má zákonodárnou moc, předkládá totiž vládě návrhy zákonů v oblasti měny, peněžního oběhu, peněžního trhu, platebního styku a vlastním postavením. V oblasti devizového hospodářství a bankovnictví předkládá návrhy spolu s ministerstvem financí. Dále má za úkol stabilizovat

[77] §7a, Zákon č. 21/1992 Sb., o bankách.
[78] Novela zákona o ČNB. *Česká národní banka* [online]. [cit. 15-3-2012]. Dostupné z: http://www.cnb.cz/cs/legislativa/konzultacni_materialy_a_navrhy/zakon_o_cnb_novela.html
[79] §25a odst. 2 Zákon č. 21/1992 Sb., o bankách.

měnu, právo vydávat bankovky a mince, řídit a organizovat platební styk a zúčtování bank, předkládat Parlamentu a veřejnosti zprávy o měnovém vývoji.

V případě zjištěného nedostatku, ČNB může kromě nápravy daného nedostatku také omezit některé povolené činnosti, jako např. zakázat provádění obchodů, převody finančních prostředků a omezení všech činností, které jsou povoleny v souvislosti s bankovní licencí, ale také může vyměnit vedoucí zaměstnance, členy dozorčí rady, zavést nucenou správu nebo uložit pokutu.

ČNB může uložit pokutu, jež je příjmem do státního rozpočtu, nejen osobám, které porušily stanovené povinnosti nebo těm, které porušily pravidla obezřetného podnikání, ale i osobám, které vykonávají činnost bez povolení a to do 50 000 000 Kč.

V případě, že pokuty a jiné donucovací prostředky nevedly k nápravě, finanční situace a likvidita je stále v rozporu se zákonnými požadavky, ČNB může rozhodnout o zavedení nucené správy. Takovéto rozhodnutí musí být řádně odůvodněno, obsahovat jméno správce, dobu po kterou má trvat nucená správa a dále musí obsahovat případná omezení přijímaní vkladů, poskytování úvěrů a pozastavení nakládání s vklady klientů[80]. Povinností ČNB je zveřejnění rozhodnutí v obchodním věstníku, poté následuje zápis do obchodníku rejstříku, kterým nucená správa nabývá účinnosti. Povinností správce je činit opatření nezbytná k obnovení stability banky, jestliže je situace natolik vážná, správce po souhlasu s ČNB může pozastavit nakládání klientů s jejich vklady, za předpokladu, že toto zmrazení povede ke stabilizaci banky. Nucená správa končí zpravidla zrušením, jakmile pominou důvody pro její trvání, pokud nebyla prodloužena a nebo pokud jí bylo odejmuto povolení působit jako banka. Rozhodnutí o zrušení nucené správy nabývá zápisem do obchodního rejstříku.

V případě, že v bance přetrvávají závažné nedostatky, může ČNB po dohodě s ministerstvem financí rozhodnout o odnětí povolení působit jako banka. Důvodů pro odnětí licence existuje více, jako např.: nepřijímaní vkladů od klientů po dobu větší než 18 měsíců, licence byla udělena na základě předložení nepravdivých údajů, v případě zahraniční banky, která ve státě svého sídla pozbyla povolení působit jako banka a v poslední řadě, jestliže banka sníží v jednom roce ztrátou základní jmění o více než 50%.

[80] SEKERKA, Bohuslav. *Banky a bankovní produkty*. Praha: Profess Consulting, 1997. 536 s. ISBN 978-80-85235-51-7.

Po nabytí právní moci rozhodnutí, banka již nesmí přijímat vklady, poskytovat úvěry a provozovat jiné činnosti, které jako banka měla povoleny.

6.3 Zákon o platebním styku

Zákon o platebním styku, který byl vyhlášen v září 2009 ve sbírce zákonů[81], dále jen ZPS nahradil zákon z roku 2002[82] přináší změny především do právní úpravy platebních služeb. Avšak i tento zákon byl změněn ve znění zákona č. 156/2010 Sb.,

Hlavním cílem tohoto zákona je transpozice nové směrnice o platebních službách[83]. ZPS obsahuje komplexní úpravu poskytování platebních služeb, vydávání elektronických peněz a provozování platebních systému. Zákon obsahuje jak podmínky pro získání příslušných povolení, tak pro činnost jednotlivých institucí a jejich dohled, který bude vykonávat ČNB. Nová právní úprava vychází z nutnosti zvýšení spotřebitelské ochrany a snahy posílit stabilitu platebních institucí a institucí elektronických peněz.

Mezi největší priority novely patří především vyřešená situace při ztrátě karty. Tentokrát je držitel ztrátu povinen bez zbytečných odkladů oznámit bance. Dříve tato povinnost byla uveřejněna pouze v obchodních podmínkách, nikoliv v zákoně. A za tuto povinnost si banka nebude smět účtovat poplatek. Při zneužití karty se podílíte s bankou,a to ve výši 150 EUR za neautorizovanou platbu. Za největší přínos úpravy zákona o platebním styku považuji zkrácení doby převodu peněz mezi účty ze tří dnů na dva. Novela také zpřísnila bankovní povinnosti jednak v nutnosti informovat klienty o transakcích na běžném účtu, a to v nejvýše měsíčním intervalu a také snížila výpovědní lhůtu smlouvy o běžném účtu, která nově nesmí být delší než jeden měsíc.

Česká republika zaznamenala prudký rozvoj bankovnictví ve všech jeho oblastech v roce 1990. Platební styk nebyl výjimkou a nastala po jeho službách obrovská poptávka. Vznikaly nové možnosti platebního styku, např. platební karty, šeky, trvalé příkazy, obstarávání inkasa atd. V rámci zvyšujícího se turismu rostl význam směnárenské činnosti a hlavně zájem o zahraniční platební styk,

[81] Zákon. č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb.,
[82] Zákon č. 124/2002 Sb., o platebním styku, ve znění pozdějších předpisů.
[83] Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitrním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES.

který do jisté míry ovlivnil vznik nové evropské měny (EUR). Před vstupem do EU v roce 2004 v České republice probíhala celá řada kroků nutných k harmonizaci právních předpisů ČR a EU. Právě před vstupem našeho státu do Evropské unie bylo vydáno několik předpisů, které bylo nutno transponovat do právních řádů vybraných oblastí platebního styku. ZPS je systematicky rozdělen do šesti částí: První část s názvem: obecná ustanovení, vymezuje předmět úpravy a základní pojmy. Část druhá - platební instituce, která upravuje podmínky pro získání povolení k činnosti platební instituce, pravidla pro poskytování platebních služeb, výjimky z obecného režimu pro poskytovatele platebních služeb malého rozsahu a dohled nad poskytováním platebních služeb. Dále jsou v této části upraveny instituce elektronických peněz, podmínky pro jejich činnost a pro vydávání elektronických peněz, výjimky z obecného režimu. Část třetí se zabývá platebními systémy, pravidly pro jejich činnost a dohled. Ve čtvrté části jsou upraveny požadavky na smlouvy o platebních službách a odpovědnost poskytovatelů platebních služeb. Část pátá pojednává o správních deliktech v oblasti platebních služeb, vydávání elektronických peněz a platebních systémech. Část šestá obsahuje především úpravu přechodného období[84].

ZPS se vztahuje se jak na bankovní tak nebankovní subjekty, to vyplývá z jeho počátečních ustanovení první části, kde je stanoveno, že „podle tohoto zákona postupují banky, pobočky zahraničních bank a jiné osoby, které provádějí nebo zprostředkovávají převody peněžních prostředků jako podnikání“[85]. Právě použitím sousloví „jiné osoby“ odděluje nebankovní subjekty provozující právě platební systémy od bank a poboček zahraničních bank.

Platební styk je jeden ze základních služeb poskytovaný bankami. Jsou to hotovostní i bezhotovostní transfery peněžních prostředků mezi fyzickými i právnickými osobami na území daného státu, ale i za jeho hranicemi[86].

O platební styk má za úkol pečovat ČNB, zajišťovat tak jeho hospodárnost a plynulost. Právní předpis, který dopodrobna upravuje platební styk a elektronické peníze je zákon č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb., který implementuje předpisy Evropských společenství[87], týkajících se platebních systémů, vypořádání obchodů s cennými papíry, institucí

[84] Zákon. č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb.,
[85] §1 písm. a) zákon č. 284/2009 Sb., o platebním styku.
[86] SCHLOSSBERGER, O. SOLDÁNOVÁ, M. a kol.: *Platební styk*, Praha.: Bankovní institut, 2007. 315/435 s. ISBN 80-7265-072-6
[87] Směrnice EP a Rady 98/26/ES, 2000/46/ES, 2007/64/ES,

elektronických peněz či o platebních službách na vnitřním trhu. Platební styk je dále upraven v zákoně č. 6/1993 Sb., o ČNB a obchodním zákoníku[88], kde je především upraven vztah mezi bankou a klientem při vedení běžného účtu. Mimo jiné, aby byla smlouva bezchybná musí obsahovat přesné označení smluvních stran, datum zřízení účtu, měnu účtu a cenu za kterou je účet zřízen.

Zákon č. 284/2009 Sb., o platebním styku především upravuje činnost některých osob, které jsou oprávněny poskytovat platební služby a vydávat elektronické peníze. Dále upravuje účast v platebních systémech, práva a povinnosti poskytovatelů platebních služeb a vydavatelů elektronických peněz[89].

Platební služby upravuje §3 zákona o platebním styku a rozumí se jím jakákoliv služba, při které dochází k vkládání nebo výběru hotovosti z účtu nebo na účet vedený poskytovatelem nebo převedení peněžních prostředků z podnětu plátce či z podnětu příjemce.

Co jsou elektronické peníze vymezuje §4 téhož zákona, jedná se o peněžní hodnotu, která představuje pohledávku za vydavatelem elektronických peněz, je uchovávána elektronicky a neměla by být přijímána proti jiným prostředkům v hodnotě nižší než je hodnota el. peněz.

Subjekty oprávněné poskytovat platební služby mohou být na základě licence jen ty, které jsou vymezené v §5 zákona výše zmíněném. Jsou to: banky, jak domácí tak zahraniční, spořitelní a úvěrní družstva, domácí i zahraniční instituce elektronických peněz[90], vydavatelé el. peněz malého rozsahu[91], domácí i zahraniční platební instituce[92] a Česká národní banka. Požadavky na udělení licence těchto institucí od ČNB se často shodují s požadavky povolení pro podnikání bank. Česká národní banka klade důraz především na právní formu podnikatelské osoby, vypracovaný obchodní plán, řádný a obezřetný kontrolní systém, důvěryhodné vedoucí osoby, účetní uzávěrku ověřovanou auditorem.

Podmínky pro udělení povolení se liší především ve výši počátečního kapitálu. Platební instituce musí mít základní kapitál 20 000, 50 000 nebo 125 000 eur, záleží na náročnosti platebních služeb, přesně tuto problematiku upravuje §16

[88] Zákon č. 513/1991 Sb., obchodní zákoník (§708-715)
[89] §1 zákon. č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb.,
[90] Instituce elektronických peněz jsou akciové společnosti, které jsou oprávněny vydávat elektronické peníze na základě povolení od ČNB. Nesmí poskytovat úvěry.
[91] Vydavatel el. peněz malého rozsahu je oprávněn vydávat el. peníze pouze tehdy, jestliže platební prostředek nepřesahuje částku 150 eur a celková výše závazků nesmí přesáhnout 5 000 000 eur.
[92] Platební instituce jsou právnické osoby, které jsou oprávněny poskytovat platební služby na základě povolení od ČNB.

Zákona č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb., Počáteční kapitál Instituce elektronických peněz musí činit alespoň 1 000 000 eur a základní kapitál u obchodní bank, jak jsem napsal výše nesmí činit méně než 500 000 000 Kč. Důvody pro odejmutí licence u institucí platebních služeb jsou také téměř shodné jako u bank. Dochází k tomu především při opakovaném a závažném porušení povinnosti stanovené zákonem.

6.4 Právní úprava elektronických peněz

Peníze elektronické povahy v širším slova smyslu nahrazují použití peněz v papírové podobě. Jedná se o peněžní hodnoty, které:

1) představují pohledávku za vydavatelem,
2) uchovanou na elektronickém peněžním prostředku
3) vydanou proti přijetí peněžních prostředků v hodnotě, ne nižší než hodnota vydávaných elektronických peněz
4) a jsou přijímány vydavatelem samotným ba i jinými osobami[93].

Aby se tedy jednalo o el. peníze, musí být splněny všechny tyto podmínky. Je důležité se zmínit, že el. peníze musí být uchovávány, po případě přenášeny peněžitým prostředkem.

Jopek dělí el. peníze do dvou druhů, podle jejich umístění.

- elektronické peníze na fyzicky existujícím samostatném nosiči
- elektronické peníze uchované v paměti počítače[94]

Existují i elektronické peníze, které mohou být uchovány na obou místech současně, tedy jak v paměti počítače, tak na přenosném nosiči. Nutno také rozlišit peněžní hodnoty, které se jeví jako el. peníze ale nejsou. Peněžní hodnota, která je zpřístupňována pomocí prostředků vzdáleného přístupu k peněžní hodnotě, však sama o sobě není elektronickými penězi.

Tyto peníze nejsou uchovávány na elektronickém peněžním prostředku[95]. Představují pohledávku za vydavatelem, ale neprobíhá zde proces přijímání

[93] §4 Zákon. č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb.,
[94] Jopek, D. *Veřejnoprávní regulace bezhotovostních plateb v ČR*. Rigorózní práce, Katedra správní vědy, správního práva a finančního práva, Právnická fakulta, Masarykova univerzita, 2006, 120 s.
[95] K tomuto více v kapitolách 2.2.4 Platební karty a 2.2.5 Elektronické peníze v Evropská centrální banka. *Modrákniha – Platební styk v České republice* [cit. 18.3.2012]. Dostupný z:

peněžních prostředků a odpovídající vydávání elektronických peněz. Prostředky vzdáleného přístupu k peněžní hodnotě také jsou obvykle přijímány jako platební prostředek širším okruhem osob, nikoli pouze jejich vydavatelem (přijímají je např. všechny banky a jiné osoby provozující terminály působící na území státu vydavatele). Jsou tedy splněny definiční znaky elektronických peněz 1) a 4), nejsou však splněny znaky 2) a 3). Mezi výše uvedené peněžní hodnoty se řadí například peněžní prostředky na běžných, vkladových, termínovaných, úvěrových a jiných účtech u bank, spořitelních a úvěrních družstev i dalších subjektů, které tedy nejsou elektronickými penězi, ale jejich alternativou. Z výše uvedeného také vyplývá, že např. předplacená karta pro stravování ve školní jídelně není elektronický peněžní prostředek a jejich vydávání tedy nepodléhá povolení od ČNB jako vydáváni el. peněz.

Zákon opravňuje vydávat el. peníze jednak banky, družstevní záložny, obdobné zahraniční instituce, instituce a vydavatele elektronických peněz. Dále může vydávat el. peníze také ČNB. Mezi podmínky pro udělení licence patří: právní forma akciové společnosti nebo evropské společnosti, základní kapitál odpovídající nejméně 1 mil. EUR, nutnost kvalifikovaných a důvěryhodných vedoucích osob. Povinnosti institucí elektronických peněz jsou upraveny velmi nestandardně odkazem na číselné označení řady ustanovení zákona o bankách[96] s uvedením "přiměřeně" pod celým odkazem. Pro určení, co je přiměřené, nestanoví ZPS žádné doplňující kritéria, která by pro instituce elektronických peněz poskytla více právní jistoty. § 52 ZPS stanoví, že instituce elektronických peněz podléhají při výkonu své činnosti dohledu ČNB. Oprávnění ČNB při výkonu dohledu jsou opět odkazem na přiměřené použití zákona o bankách.

Hlava IV. Zákona o platebním styku dále definuje, ukládá podmínky a oprávnění vydavatelům elektronických peněz malého rozsahu. §54 ZPS říká, že vydavatel musí být oprávněn vydávat el. peníze na základě zápisu do registru vydavatelů el. peněz malého rozsahu. Předpokladem pro tuto registraci je předložení adekvátního obchodního plánu a bezúhonnost. Poté může vydávat platební prostředky, které uchovávají el. peníze nejvýše v částce odpovídající 150 EUR, v celkové výši vydaných el. prostředků v jednom členském státě nepřesahující 6 mil. EUR. Takto vydané elektronické peníze jsou přijímány jako platební prostředek pouze omezeným okruhem poskytovatelů služeb, kteří mají

---

http://www.cnb.cz/m2export/sites/www.cnb.cz/cs/platebni_styk/modra_kniha/download/modra_kniha_text_2007_srpen.pdf.

[96] Zákon č. 21/1992 Sb., o bankách

úzkou vazbu na tuto osobu[97]. Dohled nad činností vydavatelů el. peněz malého rozsahu vykonává ČNB ve stejném rozsahu jako u platební instituce.

6.5 Zákon o finančním arbitrovi

V zemích EU, ale i mimo ni je kladen velký důraz na ochranu spotřebitele v oblasti bankovnictví. Není divu, vždyť v bankovnictví je klient je považován za stranu neprofesionální, který spotřebovává nabízené služby, u kterých předpokládá, že je obdrží v nabízené kvalitě, řádně a včas. Důležitým legislativním naplněním předpokladu zákona o platebním styku je právě zákon č. 229/2002 Sb., o finančním arbitrovi, který upravuje mimosoudní urovnání sporů, vznikající mezi provozovateli služeb podle tohoto zákona. Instituce finanční arbitra vznikla na základě požadavku čl. 10 směrnice 97/5/ES, vychází z teze, že soud a jeho ochrana není v mnoha případech dostatečně efektivní, protože náklady řízení v určitých případech převyšují částku sporu a navíc je soudní řízení příliš složité a neúměrně k částce.

Zákon č. 229/2002 Sb., je převážně novým právním předpisem v této oblasti, a to díky novele z roku 2011. Je zformulován tak, aby chránil tu slabší stranu, která je ve smluvním vztahu s bankami. Slabší stranu proto, že na druhé straně stojí profesionálové, kteří velmi dobře rozumí svému řemeslu a samotný spotřebitel je pouze laik, který o konkrétních produktech neví vůbec nic.

Finanční arbitr je fyzická osoba, která nerozhoduje spory pouze v oblastech platebního styku a elektronických platebních službách, ale např. i v oblastech hypotečního bankovnictví, spotřebitelských úvěrů, pojištění atd. Řízení může být zahájeno jen na návrh klienta a nesmí přesahovat částku 50 000 EUR.

Nespadá pod žádný státní úřad ani orgán či právnickou osobu. Volí ho na dobu pět let Poslanecká sněmovna na návrh ministra financí s možností znovuzvolení, dále PS volí jeho zástupce, který přejímá úřad v době jeho nepřítomnosti. Jak arbitr, tak jeho zástupce by měli být způsobilý k právním úkonům, dostatečně kvalifikováni a zkušeni v oboru, chybět by neměla ani jejich dobrá pověst. Pokud v průběhu svého mandátu ztratí způsobilost vykonávat funkci arbitra, Poslanecká sněmovna je může odvolat. I když o jeho postavení žádný předpis nic neříká, můžeme ho přirovnat k veřejnému činiteli. Po novele z roku 2011 se o

[97] §53 Zákon č. 284/2009 Sb., o platebním styku

financování úřadu FA čerpá ze státního rozpočtu, dříve financování bylo v režii ČNB.

Jak už jsem napsal výše, řízení se zahajuje na návrh spotřebitele, aby byl návrh přípustný, musí spadat do působnosti finančního arbitra a ve věci již nesmělo být rozhodnuto soudem či rozhodčím soudem nebo již řízení probíhá. Aby nedocházelo k formálním nedostatkům v návrhu, FA poskytuje formulář pro zahájení řízení. Pokud i tak je se sepsáním formuláře navrhovatel bezradný, FA musí poskytnout individuální pomoc při sepisování žádosti. Po jejím podání, musí o věci být rozhodnuto bezodkladně, případně do 15 dnů. Arbitr není vázán podle návrhu navrhovatele, rozhoduje podle svého nejlepšího vědomí a svědomí, nestranně, spravedlivě a pouze podle zjištěných skutečností. Po vydání nálezu je možné zvláštní opravné řízení, aby se hned nemusel zatěžovat soud, existuje opravné řízení přímo před arbitrem a na základě námitek je možno nález změnit nebo potvrdit. Ovšem vždy existuje možnost soudního přezkumu pro obě strany sporu, který se řídí zákonem č. 41/1963 Sb., občanský soudní řád ve znění zákona č. 151/2002 Sb.

Pokud spor žalovaná strana prohraje, finanční arbitr bance či jiné finanční instituci musí uložit pokutu ve výší 10% sporné částky, minimálně však 10 000 Kč. Pokuta je dnes příjmem státního rozpočtu. Statistiky říkají, že většina návrhů je před zahájením řízení stažena samotným navrhovatelem, z toho vyplývá jejich preventivní funkce. Arbitr vede seznam institucí na které si poškození mohou stěžovat, seznam je veden v el. podobě a naplňuje tím další funkci, tedy informativní.

Řízení u finančního arbitra může být zahájeno pouze na návrh spotřebitele, držitele elektronického platebního prostředku či uživatele platebních služeb. Podání návrhu na zahájení řízení má pak obdobné účinky jako podání žaloby na obecný soud. Poskytovatelé finančních služeb nemohou podávat návrh na zahájení řízení u finančního arbitra, a to ani vůči svým klientům ani vůči sobě navzájem. Finanční arbitr rozhoduje spory v rámci soukromoprávní agendy. Nedoplňuje pravomoci dozorových orgánů a případné dílčí otázky, např. neplatnost ujednání ve smlouvě o spotřebitelském úvěru, které by mohly zakládat odpovědnost za správní delikt dle příslušných právních předpisů, řeší finanční arbitr jen a pouze s ohledem na konkrétní jím řešený případ. Pokuty udělené finančním arbitrem instituci na základě Zákona jsou pak svou povahou spíše

institutem obdobným § 53 občanského soudního řádu (pořádkové opatření ukládané soudem)[98].

Všechny subjekty, které nyní spadají do pravomoci finančního arbitra, jsou povinny plnit vůči finančnímu arbitrovi informační povinnost, a to nejpozději ke dni, od něhož je instituce oprávněna vykonávat svou činnost. Instituce, na něž se bude vztahovat znění zákona po Novele, musí tuto povinnost splnit do 3 měsíců ode dne nabytí účinnosti Novely. Rozsah předávaných informací je blíže upraven v § 19 Zákona a zahrnuje mimo jiné také určení kontaktní osoby pro styk s finančním arbitrem a jejího zástupce. Za nesplnění této povinnosti může finanční arbitr podle povahy a závažnosti uložit instituci pokutu až do výše 1 000 000 Kč, a to i opakovaně[99].

6.6 Zákon Směneční a šekový

Zákon č. 191/1950 Sb. byl publikován, jak už je zřejmé z jeho názvu, v roce 1950 jako zákon směnečný a šekový. Navazoval na uzavření tzv. Ženevských konvencí, ke kterým se připojilo i tehdejší ČSR. Zákon je členěn do dvou základních částí, první pojednává o směnkách a druhá o šecích. Dnes v ČR šek hraje pouze podřadnou roli, je vytlačován moderními instrumenty, zejména platebními kartami nebo elektronickými převody.

[98] RUTAR, Radka. Novela zákona č. 229/2002 Sb, o finančním arbitrovi – ochrana spotřebitele?. *Www.epravo.cz* [online]. [cit. 27-3-2012]. Dostupné z: http://www.epravo.cz/top/clanky/novela-zakona-c-2292002-sb-o-financnim-arbitrovi-ochrana-spotrebitele-74566.html

[99] Tamtéž

7 Závěr

Cílem této diplomové práce je analýza elektronického bankovnictví jako celku. Na základě získaných informací, jsem se v hlavní části této práce snažil vytvořit odpovídající model současného elektronického bankovnictví, se zaměřením na vymezení jednotlivých druhů, jejich chronologický vývoj obohacený o historické zajímavosti a platnou právní úpravu dané problematiky. Nejen v této části práce jsem kladl značný důraz na technologický pokrok, který tuto problematiku od samého počátku provází, na jeho pomalý start, současný stav, ale i na raketově rostoucí technologický vývoj s výhledem do budoucna. Každá z uvedených technologií elektronického bankovnictví je podrobně popsána s ohledem na její klady, zápory, vývoj a v poslední řadě bezpečnost.

Další část se věnuje velmi důležitému tématu elektronického bankovnictví, a to platebnímu styku. Podle mého názoru, platební styk je jednou z podstatných funkcí banky, jehož hlavní ideou je bezpečné a rychlé provádění plateb. Toto téma je velmi rozsáhlé a zahrnuje jak hotovostní, tak i bezhotovostní platební styk, proto jsem do mé diplomové práce vybral pouze jednu kategorii, která má k elektronickému bankovnictví mnohem blíž, a to platební styk bezhotovostní. Snažil jsem se nastínit, jak spolu navzájem národní, ale i mezinárodní banky komunikují a na základě jakého sytému je zprostředkována komunikační výměna, proto se tato kapitola převážně věnuje mezinárodní telekomunikační síti S.W.I.F.T..

Dnes stále více lidí propadá nákupu přes internet, jak v klasických internetových obchodech, tak v aukčních síních. Za takové zboží se musí určitým způsobem zaplatit. Existuje mnoho způsobů, jak provést platbu, avšak jeden z nejbezpečnějších a nejrychlejších způsobů je prostřednictvím internetového nebankovního systému, proto jsem také zařadil tuto důležitou kapitolu do své práce. Internetové nebankovní platební systémy typu PayPal určitě mají své místo na trhu. Netroufám si říci, jakou budoucnost mají tyto společnosti, ale pokud jejich vývoj půjde tak strmě nahoru i nadále, můžeme se těšit, že 21. století bude patřit právě nebankovním systémům.

V neposlední řadě jsem se zabýval velmi aktuálním tématem, a to podvody páchanými v rámci elektronického bankovnictví. Definoval jsem nejběžnější formy protiprávních jednání v této oblasti, které ve své podstatě vždy směřují k získání citlivých údajů a následovného čerpání finančních prostředků. Je nutné si

uvědomit, že moderní technologie s sebou nesou i nové druhy trestné činnosti, jejich sofistikovaná, agresivnější povaha stále více ztěžuje jejich odhalení. Právě odcizená data, představují značný problém, především v tom, že oběť mnohdy ani nemá tušení, že byla napadena. Můžeme jen do budoucna spekulovat o dalším vývoji bankovních podvodů, stejně tak jako můžeme donekonečna spekulovat o ekonomické krizi, která má značný vliv na trestnou činnost obecně. V průběhu této kapitoly jsem se zmínil o pachatelích bankovních podvodů, ve většině případů to jsou nadměrně inteligentní, vysokoškolsky vzdělané osoby. Proto můžeme přímo úměrně předpokládat, jak moc se bude ekonomická krize dotýkat sektoru informačních a telekomunikačních technologií, kde např. může vzniknout mnoho nezaměstnaných expertů, zvyklých na vysoký životní styl, kteří v kombinaci s anonymním prostředím internetu mohou představovat veliké riziko. To je však myšleno velmi obrazně.

Mnoho z nás ani netuší, kolik možností se otevírá pro organizované zločinecké skupiny, které mnohdy čekají na chybu uživatelů elektronického bankovnictví. Myslím si, že podvody v bankovnictví se v blízké době nepodaří zcela vyhladit, o eliminaci se snaží různá bezpečnostní opatření, které však dříve nebo později pachatelé v této oblasti prolomí. Je velmi nutné mít stále na paměti, že každý potenciální uživatel elektronického bankovnictví je zároveň potencionální oběť.

8 Resumé

The aim of this thesis is the analysis of electronic banking as a whole. In the main part of this work, I trying to create an appropriate model of the current electronic banking, focusing on the definition of individual species, their chronological development, enriched with historical attractions and a valid regulation of the issue. Not only in this part of the work I put much emphasis on technological progress which is specific for a given problem. Each of these electronic banking technology is described in detail, focusing on the advantages, disadvantages, history and safety.

Another part is devoted to a very important topic of electronic banking and payment system. In my view, payment system is one of the essential functions of the bank, whose main idea is to secure and fast payment. I tried to describe, how to communicate national and international banks by SWIFT.

Internet shopping is characteristic for this time. For such goods must be some way to pay. There are many ways to make a payment, but one of the safest and fastest way is by internet non-banking system. Non-bank Internet payment systems like PayPal certainly have their place in the market.

In head section, I dealt with a very hot topic. I described the most common forms of illegal activities in this area, which aims always seek to obtain sensitive data and following these use to illegal crimes. Modern technologies carry new types of crimes, their sophisticated, aggressive nature is more difficult to detect. Throughout this chapter I mentioned the perpetrators of bank fraud, in most cases they are extremely intelligent, college-educated person.

Many of us have no idea how many possibilities are opened for organized criminal groups, they often waiting for a mistake by users of electronic banking. I think that fraud in the banking industry in the near future not completely wipe out, to help us is trying to eliminate various security measures, but sooner or later criminals will break in this area. It is very necessary to keep in mind that every potential user of electronic banking is also a potential victim.

9 Seznam pramenů a literatury

Knižní publikace:

[1] DVOŘÁK, P. *Bankovnictví pro bankéře a klienty*. 3. rozšířené vydání. Praha: Linde, 2005, Str. 371, ISBN 80-7201-515-X

[2] JOPEK, D.: *Veřejnoprávní regulace bezhotovostních plateb v ČR*. Rigorózní práce, Katedra správní vědy, správního práva a finančního práva, Právnická fakulta, Masarykova univerzita, 2006, s. 120.

[3] NOVOTNÝ, O. - ZAPLETAL, J. *Kriminologie*. 3. přeprac. vyd. Praha: ASPI, 2008. Str. 527. ISBN: 978-80-7357-409

[4] PŘÁDKA, M.: KALA, J. *Elektronické bankovnictví :* rady a tipy. Praha: Computer press, 2000. Str. 165, ISBN 80-7226-328-5

[5] SEKERKA, Bohuslav.: *Banky a bankovní produkty*. Praha: Profess Consulting, 1997. Str. 536. ISBN 978-80-85235-51-7

[6] SCHLOSSBERGER, O. SOLDÁNOVÁ, M.: a kol.: *Platební styk*, Praha.: Bankovní institut, 2007. Str. 435, ISBN 80-7265-072-6

[7] ŠENKÝŘOVÁ, B.: *Bankovnictví 1.* Praha: GRADA Publishing, spol. s.r.o., 1999. Str. 262. ISBN *80-7169-464-9*

[8] MÁČE, M.: *Platební styk klasický a elektronický*. Praha: GRADA Publishing, a.s., 2006. Str.220. ISBN 80-247-1725-5.

Časopisecké publikace:

[1] HRADECKÝ, M. – BROŽ, J. Skimming platebních karet v roce 2007. Kriminalistický sborník, 2008, roč. LII, č. 3, str. 48.

[2] KOČÍ, P.: Virtuální peníze v ohrožení. *Týden*: zpravodajský týdeník, 2008, roč. XV, č. 33, s. 45.

[3] SADOVSKÝ, D. – SUCHÁNEK, J. Platební karty a možnosti jejich zneužití. *Kriminalistika*: časopis pro kriminalistickou teorii a praxi, 2004, roč. XXXVII, č. 1, str. 29.ISSN 1210-9150.

Internetové publikace:

[1] BIC directory, seznam všech SWIFT kódů, volně přístupný na oficiálních stránkách, volně dostupných na WWW: https://www2.swift.com/directories/

[2] DOBEŠ, Pavel. Pohoda 2008. *Programy* [online]. 2008 [cit. 27-3-2012]. Dostupné z :http://www.swmag.cz/assets/clanky/2008-03/clanek00213/upload/photo/Homebanking.png

[3] EPROM. z: *Wikipedia*: *otevřená encyklopedie* [online]. Wikimedia Foundation, 2001- [cit. 2008-24-12]. Dostupné z: WWW: http://cs.wikipedia.org/wiki/EPROM.

[4] Historie platebních karet. z: *Wikipedia*: *otevřená encyklopedie* [online]. Wikimedia Foundation, 2001- [cit. 2010-18-3]. Dostupné z: http://cs.wikipedia.org/wiki/Historie_platebn%C3%ADch_karet

[5] Platební karta: *Wikipedia*: *Otevřená encyklopedie* [online]. [cit. 20-3-2012]. Dostupné z: http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta

[6] ROTTOVÁ, S. Jak moc se používá internetové bankovnictví ve světě. *Www.finance.cz* [online]. 2011 [cit. 2011-01-08]. Dostupné z: http://www.finance.cz/zpravy/finance/319968-jak-moc-se-pouziva-internetove-bankovnictvi-ve-svete-/

[7] RUML, M. PayPal konkuruje našim bankám. *Www.finance.cz* [online]. 2006 [cit. 2006-07-11]. Dostupné z: http://www.finance.cz/zpravy/finance/80569-paypal-konkuruje-nasim-bankam/

[8] RUTAR, Radka. Novela zákona č. 229/2002 Sb, o finančním arbitrovi – ochrana spotřebitele? *Www.epravo.cz* [online]. [cit. 27-3-2012]. Dostupné z: http://www.epravo.cz/top/clanky/novela-zakona-c-2292002-sb-o-financnim-arbitrovi-ochrana-spotrebitele-74566.html

[9] SKOK, P. Poradce pro platební karty. *Měšec.cz* [online], 2004, [cit. 12.1.2004]. Dostupné z: http://www.mesec.cz/poradna/platebni-karty-zima-2004/259/

[10] SWIFT User handbook, září 2003. Dostupné z WWW: http://www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2005/61180/swift_user_handbook_available_online.page

[11] VICHEREK, Roman. Padělání a pozměňování platebních karet z trestněprávního hlediska. *Www.justic.cz* [online]. [cit. 14.9.2004] Dostupné z: http://trestni.juristic.cz/524757/clanek/trest3.html

[12] Www.eurostat.ec: Využívání internetového bankovnictví ve světě: věk 16-74 let. [online]. 2011

[13] Www.paypal.cz: poplatky za platby. [online]. Dostupné z: http://www.paypalcz.cz/poplatky-za-platby

[14] ZÁMEČNÍK, P. Budoucnost platebních karet začíná! *Měšec* [online]. 2003, [cit. 17.10.2003]. Dostupné z: http://www.mesec.cz/clanky/budoucnost-platebnech-karet-zacina/

Právní předpisy:

[1] zákon č. 6/1993 Sb., o České národní bance

[2] Zákon č. 21/1992 Sb., o bankách

[3] Zákon č. 40/2009 Sb., trestní zákoník

[4] Zákon č. 52/1991 Sb., o státní kontrole

[5] Zákon č. 191/1950 Sb., zákon směnečný a šekový

[6] zákon č. 229/2002 Sb., o finančním arbitrovi

[7] zákona č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb.,

[8] Zákon č. 513/1991 Sb., obchodní zákoník

[9] Směrnice Evropského parlamentu a Rady 2007/64/ES

[10] Směrnice Evropského parlamentu a Rady 2009/44/ES

[11] Směrnice Evropského parlamentu a Rady 2009/110/ES

[12] Směrnice Evropského parlamentu a Rady 2009/111/ES

10 Seznam tabulek, obrázků a grafů

Tabulky:

Obrázky:

Grafy: