Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra obchodu a financí

Diplomová práce

Postavení bank v systému řízení rizika podvodů

Bc. Jan Schmiedt

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jan Schmiedt

Podnikání a administrativa

Název práce

Postavení bank v systému řízení rizika podvodů

Název anglicky

Role of Banks in fraud management system

Cíle práce

Cílem diplomové práce je zpracovat a vyhodnotit bankovní podvody v České republice, zabezpečení bankovnictví, využití oddělení compliance a činnost vybrané banky při těchto podvodech. Na základě provedených analýz, bude následně zhodnocena situace a postavení vybrané banky při předcházení a řešení bankovních podvodů v České republice.

Metodika

Teoretická část představuje zpracování teoretických východisek pro praktickou část studiem literatury a zhodnocením dosavadní úrovně poznání bankovních podvodů a kritické rešerši přístupů k jejich hodnocení.

Praktická část zahrnuje identifikaci vnějšího a vnitřního prostředí pomocí sběru dat, komparaci a následnou syntézu poznatků z oblasti bankovních podvodů. Součástí praktické části práce bude analýza zabezpečení bankovnictví, využití oddělení compliance a činnosti vybrané české banky při předcházení a řešení bankovních podvodů s cílem připravit podklady pro hodnocení a doporučení pro vedení banky.

Doporučený rozsah práce

60-80

Klíčová slova

PEST analýza, bankovní podvod, typy bankovních podvodů, oddělení compliance, zabezpečení bankovnictví

Doporučené zdroje informací

BLAHOVÁ, Naďa. *Rizika bank a jejich regulace.* Jesenice: Ekopress, 2018. ISBN 978-80-87865-47-7.

Dill, Alexander. Bank Regulation, Risk Management, and Compliance: Theory, Practice, and Key Problem Areas

Goldmann, Peter. Anti-Fraud Risk and Control Workbook

Hofmann, Stefan. Anti-Fraud-Management: Bilanzbetrug erkennen – vorbeugen bekämpfen

JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KALABIS, Zbyněk. *Základy bankovnictví : bankovnictví obchody, služby, operace a rizika.* Brno: BizBooks, 2012. ISBN 978-80-265-0001-8.

LANCE, James. Phishing bez záhad. 2007. ISBN 978-80-247-1766-1

POLOUČEK, Stanislav. *Bankovnictví.* V Praze: C.H. Beck, 2013. ISBN 978-80-7400-491-9.

Wiley finance series: The Principles of Banking

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Marek Dvořák, Ph.D., Ing.Paed.IGIP

Garantující pracoviště

Katedra obchodu a financí

Elektronicky schváleno dne 21. 2. 2024

prof. Ing. Luboš Smutka, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 2. 2024

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 31. 03. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Postavení bank v systému řízení rizika podvodů" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Marku Dvořákovi, Ph.D., Ing.Paed.IGIP za vedení a odborné rady v průběhu psaní diplomové práce. Mé poděkování směřuje také Bc. Marku Macháčkovi z Komerční banky za cenné rady v oblasti platebních podvodů a bezpečnosti v prostředí internetového a mobilního bankovnictví.

Postavení bank v systému řízení rizika podvodů

Abstrakt

Diplomová práce se zaměřuje na postavení vybrané banky v systému řízení rizika bankovních podvodů. Zaměřena je na identifikaci vnějšího a vnitřního prostředí vybrané banky v boji a prevenci proti bankovním podvodům (praním špinavých peněz a financování terorismu) a zabezpečení internetového/ mobilního bankovnictví. Hlavním cílem je prostřednictvím sběru dat, analýzy a provedením syntézy zhodnotit procesy v boji s bankovními podvody a nastavenými procesy. Teoretická část diplomové práce poskytuje ze studia odborné literatury odpovídající základ, díky kterému jsou definovány zásadní pojmy dané problematiky v oblasti bankovních podvodů a zabezpečení bankovnictví. Praktická část je již zaměřena na konkrétní finanční instituci a popisuje současně nastavené procesy v postupech vyhodnocování podezřelých obchodů/transakcí a nastolení prevence v boji proti podvodům. Na tuto část navazuje sběr a analýza dat, která je sledována za vybraná období s použitím statistik z interních aplikací. Do analýzy platebních podvodů je zakomponován trendy současné doby. V případě zjištěných nedostatků v procesech vyhodnocování obchodů a zabezpečení internetového/mobilního bankovnictví bude navrženo doporučení pro vedení banky.

Klíčová slova:

PEST analýza, bankovní podvod, typy bankovních podvodů, oddělení compliance, zabezpečení bankovnictví

Role of banks in fraud management system

Abstract

The thesis focuses on the role of the selected bank in the bank fraud risk management system. It is aimed at identifying the external and internal environment of the selected bank in preventing and preventing bank fraud and securing internet/mobile banking. The main goal, through data collection, analysis, and synthesis, is to evaluate processes in the fight against bank fraud and set-up processes. The theoretical part of the thesis provides the appropriate basis from the study of professional literature to define the fundamental concepts of a given issue in the field of bank fraud and the security of banking. The practical part is already focused on a specific financial institution and describes simultaneously set-up processes in the procedures for evaluating suspicious transactions/transactions and establishing prevention in the fight against fraud. Collection builds on this part and data analysis that is tracked over selected periods using statistics from internal applications. Current trends are encapsulated in the analysis of payment fraud. In the detected of identified weaknesses in the processes for evaluating suspicious trades and securing internet/mobile banking, a recommendation will be proposed for the bank's management.

Keywords:
PEST analysis, bank fraud, types of bank fraud, compliance department, banking security

Obsah

1 Úvod

Bankovní sektor je nedílnou součástí moderního společenského systému a hraje klíčovou roli v životě každého z nás. V době pokročilé digitalizace a každodenního spěchu jsme však jeho prostřednictvím vystavováni neustálému nebezpečí. V oblasti bankovní sféry jím jsou zejména rizika bankovních podvodů a kyberkriminality. Zmiňované podvody a kriminalita zahrnují různé praktiky, jako praní špinavých peněz, financování terorismu nebo různé formy platebních podvodů jakými mohou být phishing, kryptopodvody v různých formách. Tato rizika představují značnou hrozbu pro stabilitu a důvěru v bankovní systém jako celek.

Od roku 2019 společnost prakticky permanentně prochází od jedné krize do druhé. Nejdříve na přelomu roku 2019/2020 jsme byli součástí zřejmě největší společenské a ekonomické krize od II. světové války v podobě globálního viru Covid-19. Když jsme se naučili s tímto virem žít a překonali ho, objevila se nová krize – ruská agrese na Ukrajinu. Tato agrese vůči Ukrajině poznamenala každého z nás nejen přílivem válečných imigrantů, ale také prudkým nárustem cen, včetně cen energií, a inflace.

Následkem těchto krizí a prudce se zvyšujícími se požadavky na digitalizaci ze stran uživatelů, dochází k rostoucímu nebezpečí prostřednictvím internetových sítí a v přívalu nelegálních činností v obchodu přes sociální sítě. Proti těmto rizikovým aktivitám je proto ze stran regulátorů České republiky, Evropské unie nebo celého světa potřeba neustále zlepšovat boj proti nekalým praktikám v obchodu a na internetových sítích. Za posledních několik let došlo k velkým změnám z hlediska úpravy legislativy v boji proti praní špinavých peněz a v bezpečnosti internetového a mobilního bankovnictví. Nicméně veškeré tyto kroky ze stran legislativy a vyhlášek nás neuchrání před našimi vlastními činy. Je potřeba, abychom se ochraňovali i sami využíváním prostředků pasivní bezpečnosti a omezili předávání citlivých informací o svém soukromí. Účelem této práce je proto snaha popsat nová rizika rozvíjející se v současném digitalizovaném světě a nástroje, jak těmto rizikům předcházet.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je zpracování a vyhodnocení bankovních podvodů v České republice, zabezpečení internetového a mobilního bankovnictví jako reakce na platební podvody. Následné využití oddělení Compliance a činnosti vybrané banky při detekci a vyhodnocování podezřelých obchodů z hlediska praní špinavých peněz a finančního terorismu.

Dílčím cílem je pomocí sběru dat provedení analýzy, komparace a postavení vybrané banky v procesu vyhodnocování podezřelých obchodů. Dále je také porovnán vývoj trendu v oblasti platebních podvodů. Výstupem bude připravení podkladů pro hodnocení a případné doporučení k odstranění nedostatků.

2.2 Metodika

Diplomová práce je složena z vypracování teoretická a praktické části. Teoretická část práce vychází ze studia potřebné odborné literatury. Díky studiu literatury jsou definovány základní pojmy spojené bankovních podvodů s podezřelými obchody (praní špinavých peněz a financování terorismu) a bezpečnosti elektronického zabezpečení. Nejdříve je zpracována kapitola obecné regulace a dohledu nad bankami z hlediska regulátorů. Následným krokem je regulace a dohled přizpůsobena problematice praní špinavých peněz a financování terorismu (AML/CFT). Následuje kapitola platebních podvodů, kde jsou definovány nejčastější formy podvodů prostřednictvím elektronického bankovnictví. Platební podvody obecně spadají pod kybernetickou kriminalitu. Poslední kapitolou je elektronické bankovnictví a formy možných zabezpečení. Veškeré kapitoly v teoretické části jsou základem pro praktickou část.

Metodika diplomové práce aplikuje komparaci, analýzu a syntézu získaných dat. Samostatné procesy postupu při vyhodnocování podezřelých obchodů a platebních podvodů jsou zavedenými postupy ve vybrané bance.

Součástí praktické části je několik kapitol. První kapitola obsahuje vytvořenou PEST analýzu ohledně problematiky praní špinavých peněz a zabezpečení internetového bankovnictví. Následuje vyhodnocení prevence v boji proti AML/CFT ze strany Komerční banky za rok 2023, v této části je také představena činnost mezinárodní organizace FATF za rok 2021 a 2022. Nyní následují stěžejní kapitoly praktické části. Tyto kapitoly se týkají obecných postupů při analýze a vyhodnocování podezřelých obchodů / transakcí ze strany interních oddělení Komerční banky. Představeny jsou jednotlivé možnosti vyhodnocování. V první řade může být obchod po práci analytika shledán jako nepodezřelý nebo v druhé řadě může být vyhodnocen jako podezřelý. V případě podezřelého obchodu jsou nastíněny postupy v procesu až po podání hlášení o podezřelém obchodu na Finanční analytický úřad. Pomocí sběru dat z interních systému aplikací SIRON a AMLCOM jsou analyzovány výsledky práce útvarů ve srovnání s dobou a vývojem opatření v jednotlivých problematikách. V práci je také uváděna statistika ze strany Finančního analytického úřadu.

Poslední kapitolou praktické části je analýza dat platebních podvodů v rámci Komerční banky. Tato část obsahuje popis zabezpečení elektronického bankovnictví a je rozdělena na pasivní a aktivní bezpečnost. Značnou míru na bezpečnosti bankovnictví má systém FDS, který detekuje potenciální podvody.

Pro dosažení cílů jsou využity praktické znalosti autora pomocí vlastního pozorování, který je momentálně v jednom z útvarů zaměstnán. Díky tomu může mít každodenní přístup k procesům daných problematik. Vlastní zkušenosti pomohou při zhodnocení současného stavu v oblasti podezřelých obchodů a bezpečnosti internetové sféry bankovnictví.

4 Teoretická východiska

4.1 Bankovní systém České republiky

Český bankovní systém má svou historii. Vždy se určitým způsobem bankovní systém měnila s právě aktuálním politickým režimem. Od pádu komunismu se bankovní systém České republiky proměnila. Za dob komunistického režimu (centrálně plánovaná ekonomika) byl pouze jednostupňový bankovní systém, který se dal označit za tzv. monobankovní systém. Bankovní činnosti prováděla jen pověřená banka (Státní banka Československá) a plnila veškeré činnosti spojené s bankovním sektorem (ČNB,2018).

Bankovní systém České republiky je systémem finančních institucí a mechanismů, které slouží ke správě a přesunu peněžního kapitálu v ekonomice země. Aktuálně bankovní systém spadá do dvoustupňového systému, který je charakteristický tím, že na jedné straně stojí ČNB a na druhé banky, stavební spořitelny, penzijní fondy, úvěrové instituce a další finanční subjekty. V rámci bankovní systému existují finanční instituce, které poskytují širokou škálu bankovních produktů a služeb pro jednotlivce i podniky, a také specializované bank se zaměřením na financování, hypoteční úvěry a investice (ČNB, 2024).

Obrázek 1Bankovní systém ČR

Zdroj: Vlastní zpracování dle kapitoly 3,1.

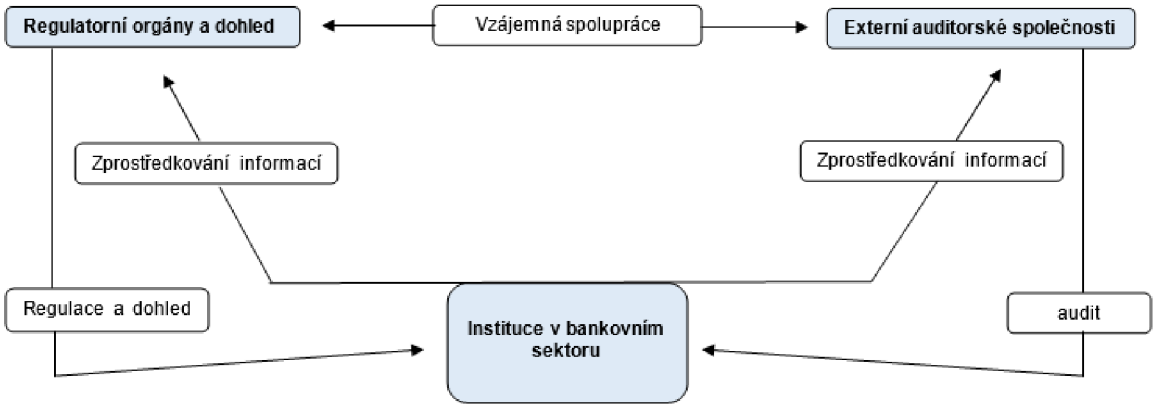
4.2 Regulace a dohled nad bankovním systémem v České republice

Regulace bankovní soustavy, jak zmiňuje ČNB (2024) vyplývá z činností České národní banky (ČNB), která současně zastává také roli centrální banky země. ČNB má za úkol dohlížet na finanční stabilitu, formulovat a provádět měnovou politiku (cenová stabilita) a regulovat bankovní sektor. Česká národní banka představuje roli orgánu, který vykonává dohled nad finančním trhem v České republice. Reguluje, dohlíží a *„Stanovuje pravidla, která chrání stabilitu bankovního sektoru, kapitálového trhu, pojišťovnictví a sektoru penzijních fondů“* (ČNB, 2024).

V současné době existují nastavená pravidla a regulace upravující činnost finančního trhu a bank. Dané instituce musí ze zákona dodržovat stanovené předpisy ČNB, a v případě nedodržování plánování z hlediska dlouhodobého výhledu či detekování podezřelých činností, mohou tyto instituce přijít o bankovní licenci. Toto jednání může mít za následek vymezení pokuty nebo vymezení sankcí jako formu postihu a v krajním případě nucený odchod z prostředí bankovního sektoru. Bankovní soustava je ovlivněna evropskými regulačními a dohledovými orgány, zejména v rámci Evropské unie a eurozóny. Odpovídající provoz a dohled nad těmito pravidly je v roli regulačních a dohledových orgánů dané země. Právě finančnictví a finanční trhy jsou jednou z nejvíce regulovaných oblastí v ekonomikách z důvodu ochrany spotřebitele a finanční stability. Součástí dohledu a regulací je i prevence proti praní špinavých peněz a financování terorismu. Bankovní regulace zahrnuje stanovení a prosazení podmínek a pravidel, kterými se banky musí řídit a dodržovat je (Revenda, 2011).

Bankovní dohled pak znamená dohled a kontrolu nad tím, jak jsou tato nastavená pravidla dodržována. Pokud jsou zjištěny odchylky od normálu, je nutné je napravit. V České republice je dohled prováděn ze strany České národní banky a následně jsou využívány také externí auditorské společnosti k ověření správnosti finančních výkazů bank a celkové činnosti. Za skutečnosti, kdy centrální banka nezaujímá dohled nad institucí, je pověřena specializovaná instituce a vykonává pozici supervizora. V rámci celého procesu je poté centrální banka v kooperaci s příslušným supervizorem a sdílí informace (Revenda, 2005).

Obrázek 2 Proces regulace a dohled nad bankami



Zdroj: Vlastní zpracování dle kapitoly 3.2

Dohled a regulace bankovního sektoru je upraven v hlavě II. zákona o České národní bance. Dohled a regulace je pro veškeré subjekty finančního trhu stejná – jedná se o veškerý trh komerčních bank a jiných finančních institucí se sídlem v ČR. Součástí dohledu ČNB jsou také investiční společnosti a veškeré činnosti spojené s obchodováním s cennými papíry (osoby, společnosti).

Dle zákona č. 335/2002 Sb., o České národní bance je součástí dohledu:

- rozhodování spojené s žádostmi o licence a registrace;
- kontrola subjektů s licencemi/ registracemi a zda jsou v souladu s dodržováním podmínek;
- kontrola činností, zda jsou v souladu s dodržováním zákonů a jinými předpisy ze strany Evropské unie;
- sběr informací potřebných k výkonu dohledu;
- rozhodnutí o opatření/postihu dle daného zákona nebo předpisů spojenými s dohledem.

4.3 Důvody regulace a dohledu nad bankami dle Mejstříka a spol.

Mejstřík a spol. (2014) odkazují na to, že regulace je zavedena proto, aby bylo možno předejít nestabilitě finančního prostředí a následné potenciální krizi. Dále Mejstříka a spol. (2014) jsou definovány základní důvody pro regulaci bank:

- **informační asymetrie;**
- **vysoká zadluženost banky;**
- **systémové riziko.**

4.3.1 Informační asymetrie

Asymetrie informací vyjadřuje nerovnováhu informací, kde určité strany mají buď více informací anebo detailnější informace než ostatní, což jim umožňuje lépe fungovat na trhu. Tato situace se vyskytuje zejména v oblasti úvěrových a pojistných trhů, kde žadatelé často disponují citlivými informacemi, což jim dává určitou výhodu nad ostatními stranami. Z hlediska společností mohou mít detailnější informace o svém finančním stavu a pozici na trhu, které nejsou veřejně dostupné. To ve výsledku znamená, že ostatní subjekty musí spoléhat na informace poskytnuté bankami nebo jinými finančními institucemi a v důsledku toho může vznikat nejistota. Jednou z nejdůležitější regulací, která se s tímto pojí, je povinnost institucí mít zajištěné povinné pojištění vkladů. To poskytuje vkladatelům větší jistotu ohledně návratnosti investic a vkladů v případě bankovního úpadku. Veřejnost, která má k dispozici pouze veřejně dostupné dokumenty jako jsou výroční zprávy nebo rozvahy, již nemá přístup k důvěrným informacím týkajícím se klientů nebo dlužníků banky. Důležitá data k větší jistotě ze strany veřejnosti, která by mohla poskytnout právě komplexnější pohled na finanční stabilitu banky, zůstávají veřejnosti nedostupná (Mejstřík, 2014).

Banky a jiné finanční a nefinanční instituce jsou vystaveny těmto rizikům:

- **negativnímu výběru**: vznik problému **před** uzavřením příslušného kontraktu (poskytnutí úvěru – subjekty, které představují vysoké úvěrové riziko);
- **morálnímu hazardu**: vznik problému **po** uzavření příslušného kontraktu (úvěr nebude použit na účel na který je sjednán – snižování schopnosti dostát z pohledu dlužníka svým závazkům) (Mejstřík, 2014).

4.3.2 Vysoká zadluženost banky

Mejstřík (2014) nahlíží na vysokou zadluženost tak, že vysoká zadluženost banky může v krajních případech vést až k úplnému pádu banky a s tím je spojeno systémové riziko (viz. 3.3.3). V případě, že jedna banka selže, může to vést k pádu dalších bank a jedním z důvodů je právě vysoká zadluženost banky. Značí se nízkým podílem kapitálu a přináší tím další potřebu regulace z pohledu orgánů. *"Rizika nesolvence a nelikvidnosti, ale i nestability bankovního sektoru prohlubuje mimořádně nízký podíl vlastního kapitálu na celkových pasivech banky. Na straně druhé jsou portfolia aktiv bank likvidnější a diverzifikovanější než u běžných firem. Potenciální křehkost sektoru je však zřejmá, což souvisí s velikou rolí, kterou v bankovnictví hraje.* (Mejstřík, 2014)"

4.3.3 Systémové riziko

Systémové riziko je v oblasti regulace a dohledu bank považováno za jedno z hlavních hrozeb stability celkového finančního systému země. Riziko vychází z možností, že selhání jedné banky nebo finanční instituce může mít dopad na celý finanční systém, a dokonce na ekonomiku jako celek. Nedostatek likvidity, způsobený nedůvěrou k bance, může mít za následek postupné rozšiřování nedůvěry mezi další finanční subjekty. V dané situaci je zapotřebí, aby prostřednictvím regulace bylo systémové riziko minimalizováno a aby byla chráněná také celková stabilita (Mejstřík, 2014).

Regulace bank z pohledu systémového rizika je možno řídit těmito způsoby:

- kapitálové požadavky – minimální rezervy;
- stresové testy – testy z hlediska postupu při extrémních situacích;
- monitorování propojenosti – propojenost mezi institucemi;
- likvidita (ČNB, 2024).

4.4 Důvody regulace a dohledu nad bankami dle M. Buckle

K odůvodnění, proč je potřeba regulovat banky je několik ekonomických a neekonomických důvodů bankovní regulace. Dle Buckle (2011) se mezi ne řadí:

- ochrana vkladatelů;

- zajištění bezpečnosti a síly banky – aby se zamezily (omezily) bankovní selhání a úpadky;
- ochrana platebního systému;
- hospodářská soutěž ve finančním sektoru.

Klady a zápory bankovní regulace ve třech oblastech:

- zranitelnost bank;
- systémové riziko;
- ochrana finančních držitelů (Buckle, 2011).

4.4.1 Zranitelnost bank

Buckle (2011) uvádí, že bankovní zranitelnost byla běžná v Evropě a USA po celou moderní dobu. Když banky začaly financovat nelikvidní půjčky prostřednictvím vkladů na vyžádání, většina recesí byla doprovázena ztrátou důvěry veřejnosti v bankovní systém, což často vedlo k nedůvěře v bankovní subjekty. Zpočátku banky soukromě vyvinuly kooperativní systémy k ochraně své kolektivní pověsti. Tyto systémy byly později přijaty a transformovány centrálními bankami, když vlády rozhodly o zavedení kontrol bankovních systémů. Navíc centrální banky začaly nabízet za krizových situací "věřitele poslední instance", kdy centrální banky působí jako konečný poskytovatelé likvidity pro banky ohrožené likviditní krizí. V nedávné době vedly centrální banky záchranné operace, při kterých „zdravé“ banky převezmou vklady „problémových“ bank.

Zranitelnost bank vyplývá z kombinace dvou faktorů:

- „run na banku“ kdy vysoký počet klientů nečekaně vybere veškeré prostředky, kterými v bance disponují – znemožní bance přístup k prostředkům na další účely podnikatelských aktivit;
- posuzování poskytování úvěrů – zda je daný dlužník schopný plnit své závazky.

Z toho plyne, že banky jsou citlivé na výkyvy důvěry veřejnosti a mohou být ohroženy v případě masového stažení finančních prostředků ze strany klientů. Dále vyplývá, že důkladné posuzování úvěrových rizik a zajištění likvidity jsou klíčovými faktory pro stabilitu bankovního systému. Centrální banky mají také důležitou roli při poskytování

likvidity v dobách krize a při řízení finanční stability. Je nezbytné, aby regulační orgány pečlivě monitorovaly bankovní sektor a přijímaly opatření k prevenci systémového rizika a ochraně stability finančního systému (Buckle, 2011).

4.4.2 Systémové riziko

Klíčovou rolí bankovní regulace, a zejména operací centrální banky, je předcházet systémovému riziku. Po tímto rizikem je možnost, že selhání jedné banky se rozšíří na jiné solventní banky. K tomu dochází proto, že vkladatelé nejsou schopni rozlišit mezi dobrými a špatnými bankami. Banka, která byla dříve solventní, se tak může stát nesolventní v důsledku svých snah generovat likviditu. V klasickém „runu na banku“ ztrácejí maloobchodní vkladatelé důvěru v schopnost své banky zůstat solventní nebo vidí problémy v jiných bankách, a proto se přidávají k „runu“ na svou banku (Buckle, 2011).

4.4.3 Ochrana finančních držitelů

Ochrana finančních držitelů neboli veřejnosti (vkladatelů) a stability platebního systému jsou důležitými důvody pro regulaci bank. Po finanční krizi se stalo problematickým rozlišit regulaci mezi bankami a investičními bankami, což vedlo k obavám o systémové riziko. Řada bank musela být zachráněna státními fondy kvůli spekulativním aktivitám, aby byly chráněny vklady a zabránilo se dalšímu šíření rizika. V nepřítomnosti jakýchkoli regulací mohou selhání bank mít hlavně dva hlavní důsledky: První důsledek je ve vztahu k selhávající bance a financování banky velice nákladný. Vysoká nákladovost se může promítnout i do ostatních bank, jelikož mezibankovní půjčky tvoří významnou část bilancí bank (Buckle, 2011).

Druhým důsledkem je přerušení platebního systému kvůli klíčové pozici bank ve správě platebního systému. Selhání bank má vážné následky, zejména kvůli specifické povaze bankovního systému. Bankovní instituce mají jedinečnou vazbu se svými věřiteli, kteří jsou zároveň jejich zákazníky. Na rozdíl od jiných firem, jejichž dluhy jsou většinou drženy profesionálními investory, jsou dluhy bank většinou drženy běžnými lidmi, kteří nemají dostatečné znalosti a informace k posouzení bezpečnosti bankovních aktiv. To znamená, že v případě selhání bank je riziko, že běžní lidé ztratí své úspory, což má vážné důsledky pro celkovou stabilitu finančního systému a ekonomiky (Buckle, 2011).

4.5 Bankovní regulace a dohled nad AML/CFT v České republice

Na regulace a dohled praní špinavých peněz a financování terorismu v České republice se dá pohlížet ze dvou úhlů.

1. Role ČNB v oblasti prevence AML/CFT

2. Úloha Finančního analytického úřadu

    a. Povinnost zabránit obchodům a transakcím, které mohou mít souvislost s trestnou činností a z toho vyplývá zastavení průtoku těchto prostředků. Shledání podezřelé operace se předává na Finanční analytický úřad (ČNB, 2024).

4.5.1 Role ČNB v oblasti prevence AML/CFT

ČNB zastává v oblasti AML/CFT tyto základní funkce:

1. **Regulace**
    a. tvorba a výklad právních předpisů (podíl na zákoně ohledně AML/CFT);
    b. vyhláška ohledně povinností v oblasti AML/CFT;
    c. role na úrovni evropské tvorby regulace.
2. **Udělování licence novým institucím na finanční trh**
    a. posuzování kritérií pro vstup na trh;
    b. původ kapitálu vznikající instituce;
    c. zavádění přísných podmínek proti zneužití postavení na trhu.
3. **Dohled**
    a. dohled nad finančními institucemi, zda dodržují platná opatření proti AML/CFT;
    b. dohled, zda je instituce schopna rizikům AML/CFT účinně předcházet
    c. dohled na dálku – sběr dat od finančních institucí a podílení se na toku informací a kooperaci mezi jednotlivými finančními institucemi.
    d. Dohled na místě – provádění kontrol pomocí inspektorů ČNB
        i. plnění povinností v oblasti AML/CFT dané legislativou a vnitřními předpisy finanční instituce

4. **Sankce**
    a. nastolení sankcí při odchylkách a zjištěných nedostatcích (legislativa, vyhlášky);
    b. forma – peněžní postih v podobě pokuty (krajním případem může být i odebrání licence) (ČNB, 2024).
    c.

Z pohledu národní úrovně probírá úzká kooperace mezi Českou národní bankou, Ministerstvem financí ČR a FAÚ. „*Spolupráce ČNB a FAÚ je rozsáhlá a spočívá mj. ve sdílení konkrétních i koncepčních informací a materiálů, koordinaci dohledové činnosti, součinnost při přípravě a výkladu právních předpisů, při přípravě Národního hodnocení rizik a dalších strategických materiálů.*“ (ČNB, 2024)

Vyhláška ČNB č. 67/2018 Sb.

předmětem úpravy je úprava *„o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření a proti legalizaci výnosů z trestné činnosti a financování terorismu („AML vyhláška“ vztahující se na instituce podléhající dohledu ČNB).“* (Vyhláška ČNB č.67/2018 Sb.)

4.5.2 Finanční analytický úřad

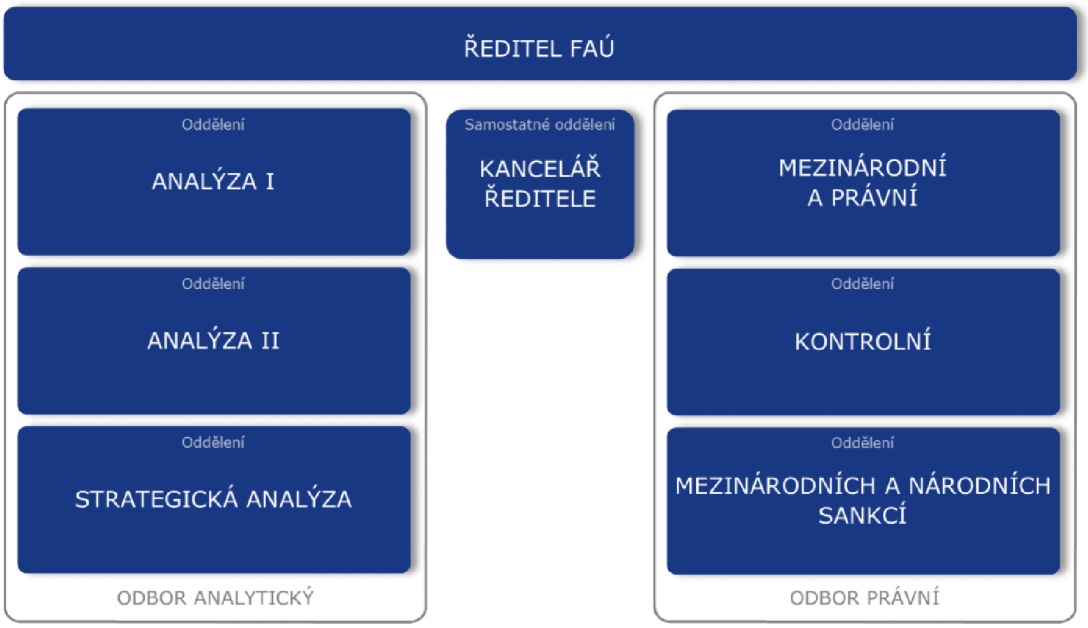
Finanční analytický úřad (FAÚ) vznikl na základě přijatého zákona č.61/1996 Sb., o opatřeních proti legalizace výnosů z trestné činnosti. Od roku 1996 zastává FAÚ roli zpravodajské finanční jednotky. Rok 2017 přinesl změny v oblasti celostátní působnosti, kdy se právě v roce 2017 stal Finanční analytický úřad samostatným úřadem. Od roku 1996 do roku 2017 zastával funkci pod záštitou Ministerstva financí. Do roku 1996, kdy byl přijat zákon č.61/1996 Sb., byla opatření proti legalizaci výnosů z trestné činnosti součástí trestního zákona č.140/1991 Sb. Právě od roku 1996 byla vůči tomuto úřadu stanovena oznamovací povinnost ze stran finančních institucí. Činnosti úřadu přímo podléhají Poslanecké sněmovně Parlamentu České republiky a kontrolním orgánem je „Stálá komise pro kontrolu činností FAÚ“. (FAÚ, 2022)

Činnosti Finančního analytického úřadu

Finanční analytický úřad má na starosti odpovědnost vůči ochraně finančního systému České republiky. Nicméně mezi nejzásadnější činnosti úřadu se řadí implementace opatření, která slouží jako prevence v boji proti praní špinavých peněz a financování terorismu (AML/CFT). Činnostmi je zodpovědný za účinnosti a výkon boje proti AML/CFT (FAÚ, 2022).

Primární činností je prevence a analytická práce ve vyhodnocování podezřelých obchodů, které jsou poskytovány ze strany povinných subjektů, především od bank. Analytická činnost spojená s podezřelými obchody je stěžejní pro následné postihy a sankce vůči subjektům, které se dopustily porušení zákona o AML/CFT. V případě podezření na nekalé obchodování a praktiky má ze zákona možnost pozastavit transakci až na 72 hodin. Lhůta 72 hodin je poskytnuta FAÚ k prošetření a v případě jakýchkoli nesrovnalostí může vést až k postoupení příslušným orgánům (Policie ČR). Tento krok oznámení o podezřelých transakcích/obchodech se přezdívá „OPO“. Oznámení o podezřelých obchodech je podáváno prostřednictvím aplikace MoneyWeb. *Hlavním účelem této aplikace je poskytnout možnost snadného a úplného podání oznámení o podezřelém obchodu (dále jen OPO) včetně možnosti využít aplikace ke vzdělávacím účelům pracovníků compliance nebo odborným útvarům, které mají v kompetenci problematiku praní špinavých peněz.* (FAÚ, 2022)“

Obrázek 3 Organizační struktura FAÚ



Zdroj: převzato z FAÚ, 2022

Obrázek 3 představuje organizační strukturu celého FAÚ, kdy nejvyšší funkci od července 2022 zastává ředitel FAÚ – Jiří Hylmar. Kancelář ředitele zprostředkovává funkci kontaktu mezi jednotlivými odděleními a ředitelem FAÚ. Analytický odbor má na starosti veškerou analytickou činnost a zastává orgán pro vyhodnocování a analýzu oznámení o podezřelých transakcích/obchodech (OPO) na území ČR. Právní odbor zodpovídá za správné dodržování a uplatňování dle kontroly AML zákona. Odbor je rozdělen na kontrolní oddělení a oddělení mezinárodních a národních sankcí (FAÚ, 2022).

4.5.3 Zákonem upravená problematika AML/CFT v České republice

Právní předpis představující problematiku praní špinavých peněz a financování terorismu je upraven v zákoně č. 253/2008 Sb. dle názvu „AML zákon“. AML zákon obsahuje stěžejní směrnice 2015/849 Evropského parlamentu a Rady (FAÚ, 2022).

Dle § 6 AML zákona je podezřelý obchod definován následovně:
„(1) Podezřelým obchodem se pro účely tohoto zákona rozumí obchod uskutečněný za okolností vyvolávajících podezření ze snahy o legalizaci výnosů z trestné činnosti nebo podezření, že v obchodu užité prostředky jsou určeny k financování terorismu, nebo že

obchod jinak souvisí nebo je spojen s financováním terorismu, anebo jiná skutečnost, která by mohla takovému podezření nasvědčovat, zejména pokud

a) klient provádí výběry nebo převody na jiné účty bezprostředně po hotovostních vkladech,

b) během jednoho dne nebo ve dnech bezprostředně následujících uskuteční klient nápadně více peněžních operací, než je pro jeho činnost obvyklé,

c) počet účtů zřizovaných klientem je ve zjevném nepoměru k předmětu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,

d) klient provádí převody majetku, které zjevně nemají ekonomický důvod, anebo provádí složité nebo neobvykle objemné obchody,

e) prostředky, s nimiž klient nakládá, zjevně neodpovídají povaze nebo rozsahu jeho podnikatelské činnosti nebo jeho majetkovým poměrům,

f) účet je využíván v rozporu s účelem, pro který byl zřízen,

g) klient vykonává činnosti, které mohou napomáhat zastření jeho totožnosti nebo zastření totožnosti skutečného majitele,

h) klientem nebo skutečným majitelem je osoba ze státu, který nedostatečně nebo vůbec neuplatňuje opatření proti legalizaci výnosů z trestné činnosti a financování terorismu,

i) povinná osoba má pochybnosti o pravdivosti získaných identifikačních údajů o klientovi, nebo

j) klient odmítá podrobit se kontrole nebo odmítá uvést identifikační údaje osoby, za kterou jedná.

(2) Podezřelým je obchod vždy, pokud

a) klientem, osobou ve vlastnické nebo řídící struktuře klienta, skutečným majitelem klienta, osobou jednající za klienta nebo osobou, která se jinak podílí na obchodu a je povinné osobě známa, je osoba, vůči níž Česká republika uplatňuje mezinárodní sankce podle zákona o provádění mezinárodních sankcí), nebo

b) předmětem obchodu je nebo má být zboží nebo služby, vůči nimž Česká republika uplatňuje sankce podle zákona o provádění mezinárodních sankcí." (zákon č. 253/2008 Sb.)

Zákon definuje mimo podezřelého obchodu také kontroly identifikace klienta a náležitosti, které jsou s tím spojené – součástí toho jsou vysvětlovány pojmy jako „politicky exponovaná osoba (PEP)“, „skutečný majitel“ a také povinná osoba, která má povinnosti ohledně oznamování podezřelých obchodů. Na § 6 AML zákona přímo navazuje § 18, který poukazuje na povinnosti oznámení podezřelého obchodu. § 18 AML zákona je definován následovně:

„(1) Zjistí-li povinná osoba v souvislosti se svou činností podezřelý obchod, oznámí to Úřadu bez zbytečného odkladu. Vyžadují-li to okolnosti případu, zejména hrozí-li nebezpečí z prodlení, oznámí povinná osoba podezřelý obchod neprodleně po jeho zjištění.

(2) V oznámení podezřelého obchodu uvede povinná osoba identifikační údaje toho, koho se oznámení týká, identifikační údaje všech dalších účastníků obchodu, které má v době podání oznámení k dispozici, informace o podstatných okolnostech obchodu a jakékoli další informace, které by mohly s podezřelým obchodem souviset a jsou významné pro jeho posouzení z hlediska opatření proti legalizaci výnosů z trestné činnosti nebo financování terorismu.

(3) V oznámení se neuvádí údaje o zaměstnanci povinné osoby nebo osobě činné pro povinnou osobu jinak než v základním pracovněprávním vztahu, která podezřelý obchod zjistila.

(4) Oznámení podezřelého obchodu přijímá Úřad. Adresu a podmínky pro doručování a další možnosti spojení pro podávání oznámení podezřelého obchodu zveřejní Úřad způsobem umožňujícím dálkový přístup.

(5) Jestliže se oznámení podle odstavce 2 týká rovněž majetku, na který se vztahuje mezinárodní sankce vyhlášená za účelem udržení nebo obnovení mezinárodního míru a bezpečnosti, ochrany základních lidských práv nebo boje proti terorismu, povinná osoba na to v oznámení upozorní. V oznámení uvede dále i stručný popis tohoto majetku, údaje o jeho umístění a jeho vlastníkovi, pokud je povinné osobě znám, a informaci, zda hrozí bezprostřední nebezpečí poškození, znehodnocení nebo užití tohoto majetku v rozporu se zákonem.

(6) Povinná osoba současně sdělí Úřadu jméno, příjmení a pracovní zařazení kontaktní osoby (§ 22) nebo osoby, která za povinnou osobu zpracovávala oznámení podezřelého obchodu, a možnosti telefonického, popřípadě elektronického spojení s touto osobou, pokud tyto informace nemá Úřad k dispozici.

(7) Zjistí-li v souvislosti se svou činností podezřelý obchod více povinných osob společně, na základě sdílení informací podle § 39 odst. 2, je splněna povinnost oznámit podezřelý obchod podle odstavců 2 až 4 všemi povinnými osobami, pokud oznámení podá alespoň jedna z nich, a v oznámení uvede, za které další povinné osoby oznámení podává.
(8) Oznámení podezřelého obchodu není porušením smluvní povinnosti mlčenlivosti povinné osoby, jejích zaměstnanců nebo fyzických osob, které jsou pro povinnou osobu činné jinak než v základním pracovněprávním vztahu. Tyto osoby nesmějí být z důvodu oznámení podezřelého obchodu vystaveny jednání, které mohou důvodně považovat za zásah do svých práv či oprávněných zájmů (dále jen „odvetné opatření")."(zákon č.253/2008 Sb.)

4.5.4 Finanční akční výbor (FATF)

Financial Action Task Force (FATF) je mezivládní organizace založená roku 1989 s činnostmi stanovujícími mezinárodní standardy proti boji praní špinavých peněz, financování terorismu a šíření nebezpečných zbraní. Jedná se o organizaci se 40 členy a 9 přidruženými regionálními uskupeními, která vydané standardy FATF dodržuje. Česká republika je členem MONEYVAL Výboru, jedním ze zmíněných regionálních uskupení (FSRB) (FATF,2024). Primární činností Finančního akčního výboru „je *hodnocení účinnosti národních AML/CFT systémů a hodnocení souladu těchto systémů s Doporučeními. Hodnocení neprovádí pouze FATF, ale taktéž jednotlivá FSRB. Hodnotící zprávy jednotlivých jurisdikcí jsou důležitým zdrojem informací, neboť mimo jiné obsahují technické informace o veřejných rejstřících, úpravě v oblasti ochrany osobních údajů, rozsahu identifikace a kontroly klienta a hodnocení rizik, kterým je jurisdikce v oblasti praní peněz a financování terorismu vystavena"* (FAÚ,2022)

4.6 Činnost oddělení Compliance v souvislosti s bankovními podvody

Oddělení Compliance představuje v činnosti banky důležitou roli. Pojem „compliance" je možné definovat jako soulad s pravidly nebo dodržování určitých pravidel. V bankovním sektoru oddělení představuje kontrolní a regulatorní orgán, který má za klíčovou roli zajišťování dodržování veškerých legislativních nařízení a regulačních požadavků.

Procesy nastavené v bance zahrnují ověřování klientů, rizikové profilování – minimalizace porušování aktivit spojených s praním špinavých peněz,
financováním terorismu, ale také dodržování jiných legislativních a etických povinností (KYC). Mezi další procesy je možné zařazení due diligence a činností s detekováním politicky exponovaných osob (Dill, 2019).

4.6.1 Oddělení KYC

Oddělení KYC „Know Your Customer“ neboli doslovně „znát svého zákazníka“. V bance je toto oddělení povinno provádět důkladné ověřování identity a hodnocení rizik klientů banky. Cílem oddělení je zajistit dostatečné informování bank o svých klientech, aby mohly identifikovat a minimalizovat rizika spojená s problematikou AML/CFT a dalšími odchylkami od legislativních norem (Dill, 2021).

Mezi hlavní funkce KYC oddělení patří:

- **Ověření identity klientů**: Provádění ověřování identity klientů v souladu s legislativním nařízením a bankovními standardy.
- **Sběr a práce s informacemi**: Potřebné informace o klientech, včetně osobních údajů, finančních informací a účelu bankovních služeb.
- **Hodnocení rizik**: Analyzování a hodnocení rizik spojených s klienty na základě profilů vytvořených při přijetí, transakcí a transakční historie.
- **Monitoring**: monitorování klientů v oblasti porušování legislativy a podezřelých obchodů.
- **Legislativní normy:** soulad mezi legislativními a regulačními požadavky ohledně informací o klientovi (Dill, 2021).

4.6.2 Due diligence proces

Dill (2021) definuje due diligence jako proces, který provádí kontrolu před uzavřením obchodní transakce nebo obchodního vztahu a průběhu vztahu z pohledu banky. Due diligence má za cíl poskytnutí dostatečné informace, zda v daném vztahu pokračovat a zda vůbec takový vztah uzavřít. Jedná se o klíčový prvek pro zajištění finanční integrity a minimalizaci rizik spojených s praním špinavých peněz a financováním terorismu.

Z pohledu banky zahrnuje proces due diligence tyto klíčové kroky:

- **Identifikace klienta**: Banka musí důkladně ověřit identitu svých klientů. Proces zahrnuje ověření osobních údajů – jméno, adresa, datum narození, a v určitých případech také ověření právního statusu a podnikatelských aktivit klienta. V tomto kroku se také informuje, zda není klient politicky exponovanou osobou.
- **Posouzení rizik**: Banka musí provést posouzení rizik spojených s novým klientem. Zjišťuje účel obchodního vztahu s klientem, hodnocení původu financí a další rizika spojená s AML/CFT.
- **Monitoring transakcí**: Banka musí dodržovat platné legislativní předpisy a vyhlášky ohledně problematiky AML/CFT. Zahrnováno je tedy splnění interních požadavků na identifikaci a přijetí klienta, analýza a hlášení o podezřelých transakcích příslušným orgánům (FAÚ).
- **Aktualizace informací**: Pravidelné kontroly a aktualizace informací o klientech banky – aktuálnost informací (Dill,2021).
-

Due diligence hraje klíčovou roli v boji proti AML/CFT, jde o proces zjišťování původu majetku a tím také prevenci AML/FCT s nelegálně získanými finančními prostředky. Proces může zahrnovat komplexní analýzu převodů, obchodů a transakcí klienta s cílem zjistit, zda se nejedné o prostředky z trestné činnosti. Důkladným zkoumáním finančních pohybů a transakcí na účtech klienta banky lze identifikovat potenciální podezřelé aktivity a obchody. V případě neobvyklých a nevysvětlitelných transakcí mohou být postoupeny na status podezřelé transakce a předány regulatorním orgánům (Dill, 2021).

4.7 Praní špinavých peněž (AML) / Financování terorismu /CFT

Evropská úprava v boji proti praní špinavých peněz je upravena směrnicí EU 2015/849, která má za cíl boj proti financování terorismu a praní špinavých peněz, stejně tak výbor FATF (kapitola 3.5.4.)

Chapman (2018) popisuje praní špinavých peněz neboli „anti-money laundering“ (AML) jako aktivitu, kdy jednotlivé fyzické osoby (FO) nebo právnické osoby (PO) zkouší zlegalizovat své finanční prostředky, které pochází z trestné činnosti (obchod s drogami, korupce, krádež, daňové úniky, podvody, úplatkářství). Cílem těchto aktivit je nabít dojmu,

že dané finanční prostředky jsou ziskem z legálních činností, které se dají potom bez rizika využívat na další činnosti.

Lze tedy říci, že praní peněz v podstatě není samotným počátečním zločinem. Praní špinavých peněz je až následkem zločinu, kdy je potřeba prostředky přetvořit na legitimní, což je samotné praní peněz.

Praní špinavých peněz je rozděleno do procesu třech činností (viz. příloha č.1):

- umístění (placement);
- vrstvení (layering);
- integrace (integration).

Finanční instituce jsou ve všech těchto fázích praní špinavých peněz zranitelné a mohou být k této činnosti zneužity. Faktory představující praní peněz mohou být: zakrytí původu, skrytí totožnosti, zajištění legálního původu. Prvním krokem je umístění, kde jsou výnosy z trestné činnosti přivedeny do procesu praní peněz. Mohou být umístěny na bankovní účet nebo do jiných finančních institucí, odkud mohou být dále distribuovány. Následným krokem je vrstvení, kdy cílem je, aby banka nebo finanční instituce spojila své jméno s legitimním zdrojem finančních prostředků, díky čemu vytváří prostor mezi trestným činem a finančními prostředky získanými z něj. Posledním článkem je integrace, kdy prostředky převedené na „čisté“ mohou být již součástí legitimních obchodů (Chapman, 2018).

Financování terorismu (CFT)

Financování terorismu neboli „combating the financing of terrorism“ (CFT) je proces poskytování a zajišťování financí nebo jiných zdrojů pro podporu činností, které jsou spojené s terorismem. Tato činnost může zahrnovat nejen finanční prostředky, ale také materiální vybavení k použití. Organizování nebo provádění teroristických činů. Typy transakcí, které by mohly sloužit k financování terorismu mohou mít podstatu:

- nevysvětleného nárůstu výběrů hotovosti, šeků nebo převodů s nízkou hodnotou;
- vklad hotovosti fyzických osob bez zjištěného zdroje příjmu;
- sbírka v rámci charitativních darů (El Khoury, 2023).

V boji proti financování terorismu musí finanční instituce věnovat jako při praní špinavých peněz zvláštní pozornost identitě původce a příjemce transakce, původu prostředků a destinaci, kam finanční prostředky putují (seznam rizikových zemí viz. příloha č.3) (European Union,2022).

4.7.1 Evidence skutečných majitelů

Dle zákona o evidenci skutečných majitelů č. 37/2021 Sb. je povinností sledovat skutečné majitele právnických osob jako prevenci proti praní špinavých peněz a financování terorismu. Skutečným majitel (ultimate beneficial owner „UBO“) se stává jakákoli fyzická osoba (FO), která je v podobě podílu zainteresována ke vztahu k právnické osobě (PO). Každá právnická osoba může mít ve vztahu skutečných majitelů více osob, nicméně skutečným majitelem zůstává pouze fyzická osoba, člověk.

Materiální skutečný majitel korporací je taková osoba, která:

- v konečném důsledku kontroluje podíl nebo podíl na hlasovacích právech alespoň s 25 %;
- má právo na podíl ze zisku společnosti nebo likvidačních zůstatcích alespoň 25 %;
- vlastní rozhodující vliv v korporaci s podílem alespoň 25 % (AML zákon č. 253/2008 Sb.).

Skuteční majitelé jsou evidováni v „Evidenci skutečných majitelů“. Evidence je informační systém veřejné správy České republiky. Evidenční povinnost je povinností každé právnické osoby se sídlem v České republice (Evidence skutečných majitelů,2023).

Obrázek 4Evidence skutečných majitelů

Zdroj: Evidence skutečných majitelů, 2024

4.7.2 Politicky exponovaná osoba

Politicky exponovaná osoba je odvozená od anglického výrazu „politically exposed person“ (PEP). Jedná se o takovou osobu, která zastává určitou politicky významnou funkci. Dále je tento termín používán v oblasti finančnictví a bankovního sektoru.

Z pohledu metodického pokynu č.7 FAÚ je politicky exponovaná osoba definována následovně: *„fyzická osoba, která je nebo v minulosti byla ve významné veřejné funkci s celostátním nebo regionálním významem (tzv. vnitrostátní PEP).“*

Funkce vnitrostátních politicky exponovaných osob:

- hlavy států nebo vlád;
- přední političtí činitelé;
- čelní představitelé vlády;
- členové řídích orgánů politických stran;
- představitelé soudních orgánů;

- představitelé ozbrojených sil;
- členové vyššího vedení podniků ve vlastnictví státu
- vedoucí představitelé územní samosprávy (primátor, náměstek primátora, tajemník)
- aj (viz. příloha č. 2) (metodický pokyn č.7 FAÚ, 2023).

Osobami, které jsou považovány za politicky exponované, mohou být i osoby, které vykonávají obdobné funkce v jiném státě anebo v orgánu Evropské unie. Označovány jsou jako tzv. zahraniční PEP (velvyslanec, vedoucí diplomatické mise). Dle definice politicky exponované osoby se za tyto osoby považují také osoby napojené na politicky exponované osoby (odvozené PEP) a těmi jsou:

- blízké osoby – rodinný příslušník, registrovaný partner;
- *„společník nebo skutečný majitel stejné právnické osoby, popřípadě svěřenského fondu, nebo osoba, která je s takovou osobou v jakémkoli jiném blízkém podnikatelském vztahu;*
- *skutečný majitel právnické osoby, popřípadě svěřenského fondu, vytvořené ve prospěch takové osoby.“* (metodický pokyn č.7 FAÚ, 2023)

V souladu s regulacemi proti praní špinavých peněz a financování terorismu (AML zákon č.253/2008 Sb.) je pro finanční instituce důležité tyto osoby identifikovat, aby mohly provádět „due diligence“, monitorovat transakce spojené s PEP. Daná opatření jsou důležitá z hlediska provádění nezákonných účelů a korupce.

Způsoby zjištění statusu politicky exponované osoby u klienta:

- při procesu přijímání klienta ve finanční instituci;
- zjištění v seznamu vnitrostátních funkcí politicky exponovaných osob;
- kooperace mezi finančními institucemi;
- prohlášení klienta při vzniku vztahu (obchodní vztah) (zákon č.253/2008).

4.8 Platební podvody

Kybernetická kriminalita z pohledu bankovních podvodů je dle mezinárodních dohod o kyberzločinu upravena ve sdělení č. 104/2013 Sb. Ministerstva zahraničí o Úmluvě Rady Evropy o počítačové kriminalitě (Úmluva o počítačové kriminalitě, 2001). Úpravu o kybernetické kriminalitě dále upravuje tzv. Budapešťská úmluva (2001 – naposledy upravena 2021). Kybernetická kriminalita často označována jako také kyberkriminalita, je forma kriminality, která se odehrává v kyberprostoru prostřednictvím počítačových sítí, internetu nebo jakéhokoli zařízení sloužící k trestné činnosti Platební podvody jsou druh kybernetické kriminality, spadající do bankovních podvodů a druhy mohou být: Phishing,vishing, smishing, , fake prezident, kryptopodvod nebo krádež identity sloužící k následnému podvodu (Jirovský, 2007).

4.8.1 Phishing

Phishing je praktika zasílání podvodných komunikací, které vypadají, že pocházejí z důvěryhodného a existujícího zdroje (banky, pojišťovny, státní správa sociálního zabezpečení, pošty). Phishing je závažný, nebezpečný a díky digitalizaci velmi častý typ kybernetického útoku.
https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing

Nejčastější formy útoku:

- podvodný email;
- SMS zpráva;
- internetový odkaz;
- webové stránky banky.

Typicky se jedná o spamové e-maily s aktivním odkazem, který má oběť „přesměrovat“ na stránku, na které se dozví o „problému“, o kterém je informováno v komunikaci s podvodníkem. Cílem je oklamat uživatele a donutit je k vyplnění osobních údajů, zadání bankovních údajů anebo nainstalování programů do svého zařízení. Důvody, proč se uskutečňují phishingové podvody, jsou různé, ale jak již bylo zmíněno, útočníci cílí na uživatelsky cenná data – získání přístupu k citlivým osobním údajům a přihlašovacím údajům do bankovnictví nebo nainstalování škodlivého programu do zařízení oběti útoku.

Nejnebezpečnější je útočníkům poskytnout data o bankovních kartách, kdy může nastat úplné okradení o veškeré finance, kterými uživatel disponuje. Do kategorie phishingového podvodu spadají také útoky pomocí telefonního hovoru (vishing) a textových zpráv (smishing) (Cisco, 2024).

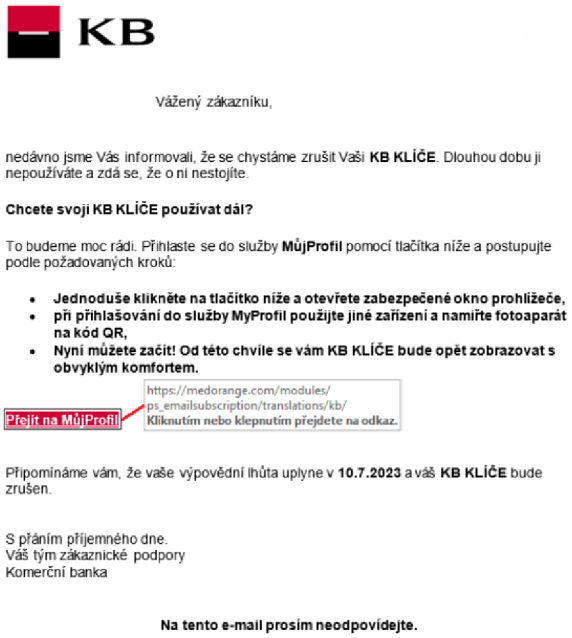
Ochrana před phishingovým útokem:

- kontrolovat adresy odesílatele e-mailu;
- nepoužívat podezřelé odkazy;
- nikdy neposkytovat osobní data;
- všímat si špatné gramatiky a nepřesností (Cisco, 2024)

Phishing se začal objevovat již koncem 20. století, kdy se internet začal dostávat mezi každodenně používané sítě. První případy se objevovaly v podobě podvodných e-mailů, kdy se primárně vydávaly za bankovní instituce. Postupným časem a vývojem se tyto kybernetické praktiky postupně stávají sofistikovanějšími a propracovanějšími, aby předešly veškerým bezpečnostním opatřením. (James, 2005)

Prvním případem phishingového útoku byla v roce 2006 banka CitiBank a její klienti. Forma útoku byla prostřednictvím e-mailu, kde stálo oznámení o přijetí finanční částky. Následoval odkaz, kde k připsáním prostředků na účet bylo potřeba vyplnit osobní údaje a přihlašovací údaje k bankovnímu účtu (Českénoviny.cz, 2006)

Obrázek 5 Typ phishingového útoku



KB

Vážený zákazníku,

nedávno jsme Vás informovali, že se chystáme zrušit Vaši **KB KLÍČE**. Dlouhou dobu ji nepoužíváte a zdá se, že o ni nestojíte.

Chcete svoji KB KLÍČE používat dál?

To budeme moc rádi. Přihlaste se do služby **MůjProfil** pomocí tlačítka níže a postupujte podle požadovaných kroků:

- **Jednoduše klikněte na tlačítko níže a otevřete zabezpečené okno prohlížeče,**
- **při přihlašování do služby MyProfil použijte jiné zařízení a namiřte fotoaparát na kód QR,**
- **Nyní můžete začít! Od této chvíle se vám KB KLÍČE bude opět zobrazovat s obvyklým komfortem.**

Přejít na MůjProfil

https://medorange.com/modules/ps_emailsubscription/translations/kb/
Kliknutím nebo klepnutím přejdete na odkaz.

Připomínáme vám, že vaše výpovědní lhůta uplyne v **10.7.2023** a váš **KB KLÍČE** bude zrušen.

S přáním příjemného dne.
Váš tým zákaznické podpory
Komerční banka

Na tento e-mail prosím neodpovídejte.

zdroj: interní materiály KB, 2023

Proč se u obrázku jedná o phishing? Hned v první větě je patrné špatné gramatické vyjádření „Vaši KB Klíče“, následuje „Chcete svoji KB Klíče“ a nejjasnějším důkazem podvodu je odkaz, který absolutně nesouhlasí s žádnou stránkou Komerční banky, a.s.

4.8.2 Vishing / Smishing

Podvody pod pojmem vishing jsou takové podvody, které mají podstatu ve phishingu. Jedná se o stejný princip s cílem získat citlivé osobní údaje, přístupy do bankovnictví a potvrzení transakce ve svém internetovém/mobilním bankovnictví. Vishing na rozdíl od phishingu je prováděn pomocí podvodných telefonátů (voice phishing). Využívána je tedy hlasová komunikace s cílem oklamání obětí (Proofpoint, 2024).

Hlavním znakem jsou brzké či pozdní časy hovoru s cílem získání osobních dat nebo bankovních údajů. Útočníci se nejčastěji vydávají za telefonní bankéře, zaměstnance ČNB nebo jiných státních organizací. Své metody mají natolik propracované, že v případě pochybností útočník zašle formou zprávy SMS, aplikace Whatsapp „pracovní průkaz“ dané banky (Policie ČR, 2021).

Obrázek 6 Typ vishingového útoku – průkazka

Zdroj: interní materiály KB, 2023

Ochranou proti tomuto typu podvodu a jak se chránit je dodržování základních doporučení – nikdy nesdělovat přístupové údaje, čísla platebních karet a jiné citlivé údaje. Při nejistotě raději ukončit hovor a zavolat později na doporučenou infolinku než sdělit údaje či potvrzovat transakce v internetovém/mobilním bankovnictví. Bankéř nikdy nebude vyžadovat žádné citlivé údaje, bankovní údaje nebo čísla karet (Komerční banka, 2023)

Smishing

Smishing neboli SMS phishing je typ podvodu ze světa kyberzločinu, který využívá manipulativní textové zprávy adresované obětem k získání citlivých osobních dat, údajů bankovních karet nebo přihlašovacích údajů do bankovnictví. Cílem smishingu je oklamání oběti a následné poskytnutí těchto údajů, které jsou využity na zcizení finančních prostředků, krádeže identity nebo jiného podvodného jednání. Stejně tak jako phishing a vishing, tak i smishing je velice rozšířeným problémem v kybernetické bezpečnosti (Forbes, 2023).

Smishing využívá textové zprávy, aby z pozice banky, úřadu nebo poštovní služby zmanipuloval uživatelel k poskytnutí již zmíněných osobních dat a bankovních údajů. Vyskytují se nevyžádané SMS zprávy, které odkazují na výhry v soutěžích nebo zadání svých osobních údajů nebo bankovních údajů k ověření nebo doručení balíků. Ochranou před tímto typem phishingu je obezřetnost a dbání ostražitosti vzhledem k zadávání údajů a dat přes odkazy, které jsou uvedené v SMS zprávě. V případě jakýchkoli nesrovnalostí je vždy dobré ověřit si informace u oficiálních zdrojů příslušné organizace (Komerční banka, 2023).

Obrázek 7 Typ smishingového útoku

Zdroj: interní materiály KB, 2023

4.8.3 Kryptopodvody

Krypto podvod je taková forma podvodu, která využívá investice v podobě kryptoměn nebo celý kryptoměnový trh k oklamání klientů bank s cílem získat finanční prostředky. Nejčastější forma krypto podvodů je formou podvodných investic. Jedná se o falešné nabídky investic či investičního poradenství s cílem vymámit od klienta platby na vlastní účty. Takovéto investice bývají většinou prováděny pomocí phishingového a vishingového útoku. Znakem těchto podvodů je podezřele lákavá nabídka investic s vysokým výnosem. Zdrojem jsou sociální sítě, e-mailové komunikace a také uměle vytvořené reklamy se známou osobností. Ochranou před tímto typem je nereagovat na nabídky vysokého výnosu a v případě, že chce klient opravdu obchodovat s kryptoměnami je nejlepší volbou obchod s ověřenými obchodníky (Komerční banka, 2023).

Součástí krypto podvodu jsou dle Komerční banky (2023) tyto scénáře dle typu provedení:

Klient reaguje na podvodnou nabídku na internetu

Klient v rámic svého zařízení reaguje na lákavou nabídku formou vysokého výnosu investic. Dříve byl klient banky instruován podvodníkem, na které účty a burzy je potřeba zasílat prostředky pro nejvyšší zhodnocení (účty podvodníků). Aktuálně je klientovi nabídnuta pomoc se založením a správou investičního účtu „plný servis“, za tímto účelem dochází k instalaci aplikace pro vzdálený přístup, kde dojde k odcizení veškerých osobních a finančních dat a následně dojde k výzvě, aby klient potvrdil v mobilním bankovnictví tranksakci související s „investicí.

Kontaktování klienta telefonicky – pomocí vishingu

Klient je kontaktován na základě sjednaného „úvěru“ například v ČSOB, klient sdělí, že takovou banku ani nemá a podvodník zjistí jaké bankovní služby a u koho využívá. Po určité době přijde kontaktování z „jeho“ banky, pod záminkou ověření a zmanipulování k odeslání prostředků a nabídce výhodného obchodu formou krypto.

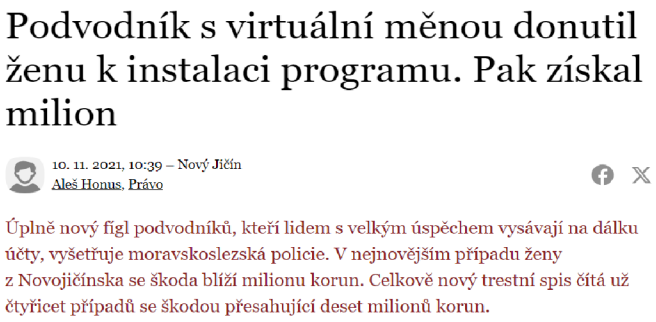
Klient plní funkci tzv. „bílého koně“

Formou klienta, který byl součástí nebo je součástí podvodu souvisejícími s investicemi do kryptoměn, je plněna funkce prostředníka v procesu přeposílání odcizených finančních prostředků. Klientovi je nabídnuta možnost kompenzace ztráty peněz z nevydařené investice tím, že bude přeposílat prostředky, které obdrží na účet od jiných klientů za částečnou úplatu nebo pod záminkou toho, že dané prostředky jsou již vráceny přímo klientovi a má je reinvestovat.

Klient je kontaktován ze strany České národní banky

Klient je obeznámen prohlášením, že jeho účet je napaden a bude mu proto zablokován a zmrazen. Dostane informace, že je nutné si veškeré prostředky vybrat a pro jejich ochranu je vložit na „bezpečnostní účet“ ČNB nebo na účet v „bitcoinmatu.“

Obrázek 8 Typ kryptopodvodu



Podvodník s virtuální měnou donutil ženu k instalaci programu. Pak získal milion

10. 11. 2021, 10:39 – Nový Jičín
Aleš Honus, Právo

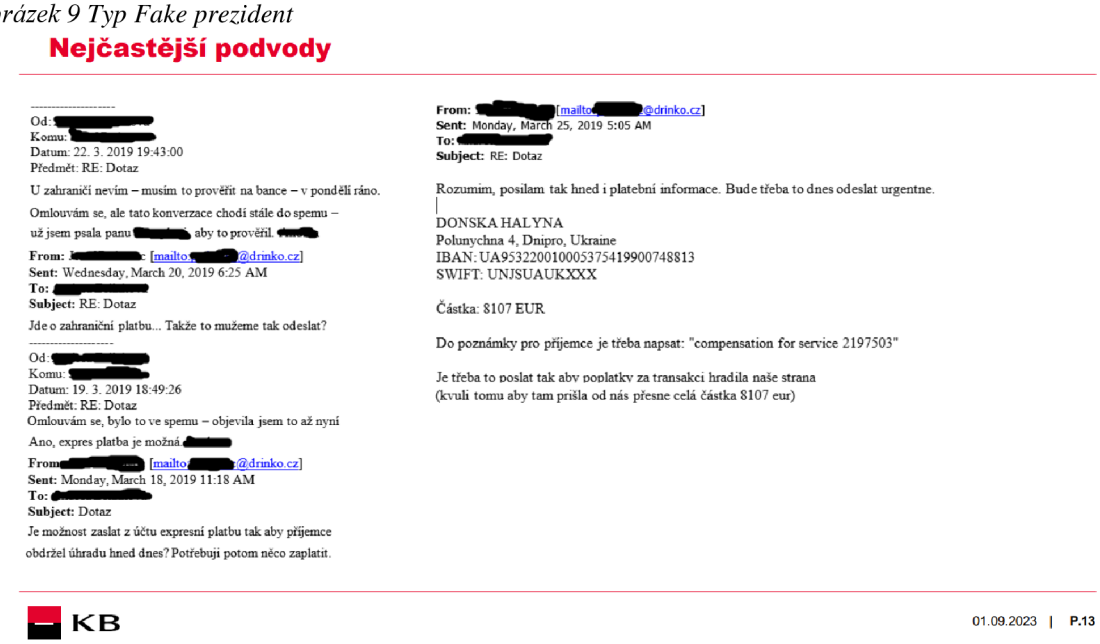
Úplně nový fígl podvodníků, kteří lidem s velkým úspěchem vysávají na dálku účty, vyšetřuje moravskoslezská policie. V nejnovějším případu ženy z Novojičínska se škoda blíží milionu korun. Celkově nový trestní spis čítá už čtyřicet případů se škodou přesahující deset milionů korun.

Zdroj: Novinky.cz,2021

4.8.4 Fake prezident

Jedná se o typ podvodu formou e-mailu či telefonu (SMS, hovor) s cílem přesvědčit podřízeného (nejčastěji) k zaslání podvodné platby (zpravidla do zahraničí). Vyznačuje se podezřelou zprávou (e-mailem) z adresy, tvářící se jako od nadřízeného. V případě dovolené nebo služební cesty nadřízeného může jít o tlak na odeslání platby co nejdříve. V komunikaci se často vyskytují nezvyklá slova či špatná gramatika. Fake rezident cílí na střední firmy s horším zabezpečením sítě, nepozorné podřízené. Chránit se před tímto podvodem lze pasivně a pouze ze strany osob, kterým je zpráva směřována. Lze využívat vícefázové ověření, vždy kontrolovat adresu e-mailu či telefonický kontakt s neznámými nadřízenými (Komerční banka, 2023)

Obrázek 9 Typ Fake prezident



Zdroj: interní materiály KB, 2023

4.8.5 Krádež identity

Krádež identity není označována zcela jako bankovní podvod, nicméně díky krádeži identity lze poté daný podvod uskutečnit. Jedná se o kriminální čin s cílem vydávat se za jinou osobu a získat díky ní finanční prostředky, osobní informace nebo jiné informace důležité pod pojem krádež identity. V případě, že se osobní údaje/čísla bankovních karet dostanou do neoprávněných rukou, může osoba rychle přijít o finanční prostředky, ale také nést odpovědnost za veškeré závazky vedené na danou osobu (úvěry, smlouvy, …). Následkem může být obvinění z trestných činů, která spáchala cizí osoba pod jménem jiné osoby. Dokázat poté skutečnost, že byla identita ukradena, je velice složité (Komerční banka, 2023)

Podoby a způsoby odcizení identity:

- **Finanční krádež** – představuje největší nebezpečí a také nejčastější. Podvodník využije osobní údaje, čísla bankovních karet nebo přístupy do bankovnictví. Důsledkem toho může podvodník spáchat platební podvod, koupit zbraně, vzít si úvěr. Z tohoto důvodu je úzké spojení mezi pouze kriminálním činem a bankovním podvodem (platebním podvodem).

- **Vystupování pod cizí identitou jiné osoby** – poskytnutí údajů v rámci osoby zapojené do trestního řízení.
- **Vytvoření zcela nové identity** (Policie ČR, 2010)

Příznaky, které mohou naznačovat, že se osoba stala obětí krádeže identity:

- nepovolené transakce/pochybné transakce;
- dokumentace – ze strany státních orgánů, bankovních institucí;
- potvrzení nebo faktury za nákupy, které osoba neprovedla (Policie ČR, 2010).

V případě těchto příznaků je důležité neodkladně informovat příslušné instituce (banky, instituce státní správy) a zahájit opatření. Prevencí je pasivní bezpečnost každého jedince. Dbát zvýšené pozornosti na své dokumenty, osobní informace a bankovní údaje. Vyhnout se platbám na neprověřených stránkách a nesdělovat nikomu své údaje (Policie ČR, 2010).

4.9 Elektronické bankovnictví

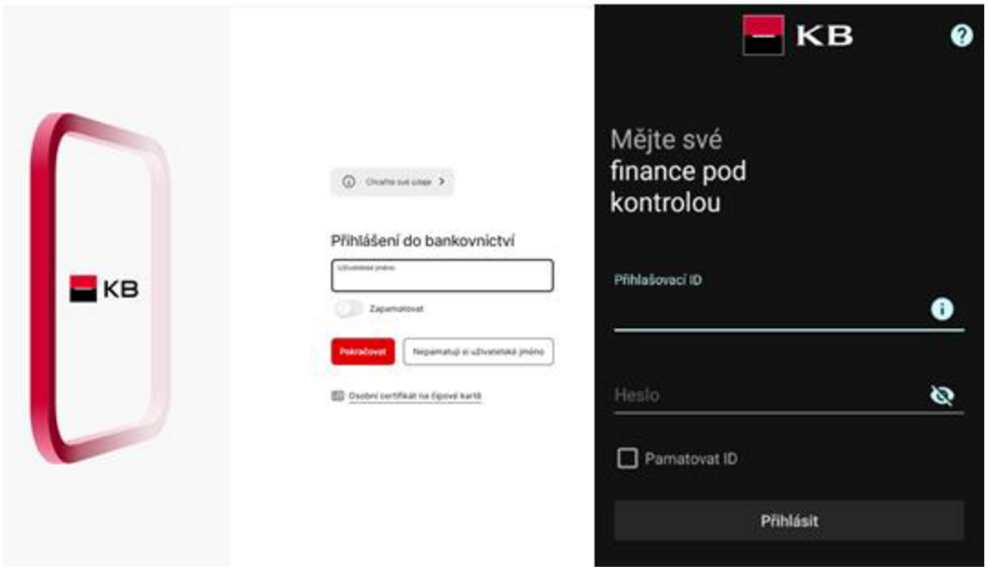
Internetové bankovnictví má spousty názvů, je označováno jako elektronické bankovnictví, e-banking nebo také jako online bankovnictví. Jedná se o službu nabízenou bankami a finančními institucemi, která umožňuje klientům správu svého bankovnictví prostřednictvím webových platforem nebo mobilních aplikací bez použití návštěvy pobočky. Online bankovnictví lze spravovat z jakéhokoli zařízení, které má přístup k internetovému připojení (nejčastěji počítač, tablet, telefon). Důvodem vzniku online bankovnictvím je především technologie a náročnost klientů. Díky vývoji doby v oblasti bankovnictví se již cílí spíše na bezkontaktní bankovnictví, které má ale zcela jistě svá rizika (Springer, 2013).

Formy elektronického bankovnictví:

- **Internetové bankovnictví**: Přístup k bankovním službám prostřednictvím webových platforem poskytovaných bankami. Slouží ke správě financí, převodům prostředků a provádění transakcí.

- **Mobilní bankovnictví**: Mobilní aplikace poskytované bankami umožňují klientům přístup ke správě bankovnictví a provádění transakčních operací pomocí mobilních zařízení (chytrý telefon, tablet). Výhodou je, že má klient přístup ke svým financím z celého světa.
- **Telefonické bankovnictví**: Provádění operací skrze telefonní hovor s bankovními zástupci (Springer, 2013).

Obrázek 10 Internetové a mobilní bankovnictví



Zdroj: Komerční banka, 2024

4.9.1 Zabezpečení bankovnictví

Zabezpečení bankovnictví je možné z hlediska banky a také z hlediska klientů. Pro banky a finanční instituce je zabezpečení zásadní prioritou. Ze strany banky je potřeba zajistit bezpečnost a ochranu osobních údajů, finančních prostředků a bankovních transakcí (Raiffeisenbank, 2024).

Opatření bank k poskytnutí bezpečnosti a ochrany:

- **Dvoufázové ověření**: Dvoufázové ověření vyžaduje před provedením jakékoli operace a přístupem k účtu ověření v podobě zadání dvou nezávislých faktorů (hesla a jednorázový SMS kód). Toto umožňuje předejít rizikovosti úniku dat a je vyžadována znalost nejen hesla.
- **Biometrické ověření**: Zavádění ověření pomocí biometrické metody – otisk prstu, Face ID nebo hlasové rozpoznávání. Jedinečnost zabezpečení z hlediska rozdílných biometrických charakteristik každého z klientů.
- **Šifrování dat**: Ochrana osobních a finančních údajů klientů (hesla, ID a finanční údaje). K šifrování dat dochází během přenosu skrz internet a slouží k zajištění zakódování dat a ochranou před neoprávněným přístupem.
- **Monitoring**: Monitorování aktivit u bankovních služeb banky – identifikování podezřelých aktivit a potenciálních podvodů. Interní systémy sledují, detekují a vyhodnocují rizikovost podezřelých transakcí a umožňují ochranu klientů před ztrátou a zneužitím (Raiffeisenbank, 2024).

Ochrana a zabezpečení ze stran klientů:

- použití bezpečných zařízení – nepoužívat veřejné počítače a WI-FI sítě;
- ochrana údajů o přihlášení;
- volba silných hesel – malá/velká písmena, znaky a čísla;
- důvěryhodné adresy internetového bankovnictví – oficiální stránky banky;
- zvýšená pozornost – podezřelé soubory a e-maily;
- kontrola aktivit v IB (Komerční banka, 2024)

4.10 PEST analýza

Podle Sedláčkové a spol. (2006) je PEST analýza nástroj používaný pro hodnocení vnějšího prostředí makrookolí a základ je tvořen z těchto čtyř faktorů:

P – politické faktory

E – ekonomické faktory

S – sociální faktory

T – technické faktory

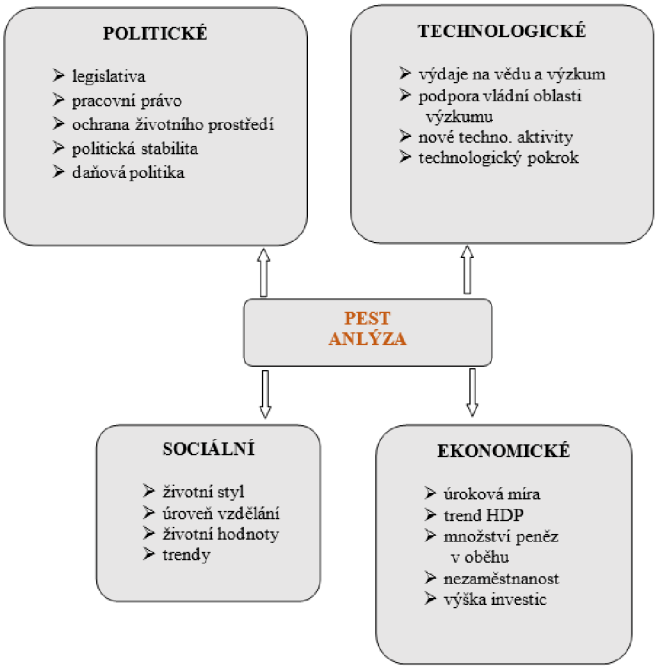
Politické faktory – zahrnují veškeré politické aspekty (vládní politiky, zákony, regulace a stability politického prostředí).

Ekonomické faktory – zkoumány jsou zde ekonomické podmínky vnějšího prostředí.

Sociální faktory – zaměření na sociální trendy, změny ve společnosti, demografické změny a životná styl.

Technologické faktory – inovace, technologické trendy a vývoj z oblasti.

Obrázek 11 PEST analýza



Zdroj: vlastní vypracování (Sedláčková; Buchta, 2006)

PEST analýza se často využívá v oblasti strategického řízení a plánování, aby mohla organizace lépe porozumět svému vnějšímu prostředí. Cílem je přizpůsobit se, porozumět potřebám, aktuálním trendům mikrookolí a pomoci identifikovat příležitosti a hrozby, které mohou organizaci ovlivnit (Sedláčková a kol., 2006).

5 Vlastní práce

Praktická část diplomové práce je rozdělena na několik dílčích částí. Nejdříve je v diplomové práci vypracována PEST analýza na prostředí banky v oblasti podezřelých obchodů a bezpečnosti elektronického bankovnictví. Druhou částí bude představení prevence a boj proti AML/CFT ze strany Komerční banky za rok 2023, dále budou následovat hlavní činnosti výboru FATF za rok 2021 a 2022. Třetí část se bude odkazovat na obecné postupy útvaru AML a AMLCOM s následnou analýzou z interních aplikací SIRON a AMLCOM. Tato část bude v poslední řadě rozšířená o činnosti Finančního analytického úřadu s analýzou problematiky podezřelých obchodů (AML/CFT). Poslední část práce bude obsahovat analýzu platebních podvodů včetně trendů a zabezpečení internetového/mobilního bankovnictví v Komerční bance, a.s.

5.1 PEST analýza

PEST analýza poskytuje základní přehled o faktorech, které ovlivňují praní špinavých peněz a zabezpečení internetového/mobilního bankovnictví z hlediska platebních podvodů. Napomáhá bankám a finančním institucím lépe porozumět vnějším faktorům a přizpůsobit svou strategii v souladu s těmito vlivy.

Politické faktory:

- Regulace a zákony: politcké předpisy a jiné legislativní regulace v oblasti kybernetické bezpečnosti mohou mát významný vliv na povinnosti bank a jiných finančních institucí v oblasti proti podvodům.
- Z oblasti AML/CFT se bezpochybně jedná o legislativní předpisy a regulace v rámci této problematiky.
- Spolupráce mezi státy a mezinárodními organizacemi jako je FATF (FSRB).

Ekonomické faktory:

- Finanční podmínky v oblasti hospodářské stability mohou ovlivnit úroveň investic do zlepšování bezpečnostního systému aktivní ochrany.
- V případě AML/CFT je hledisko sankcí a finančního tlaku, kdy mohou být omezeny finanční toky, které podporují praní špinavých peněz a fin. Terorismu
- Rozvoj finančních center;

- země s lepšími podmínkami (např. HDP) mohou připívat k lepší finanční zabezpečenosti

Sociální faktory:

- Zvyšování povědomí o rizikovosti internetového a mobilního bankovnictví a celkové bezpečnosti v oblasti bankovnictví.
- Lepší finanční gramotnost mezi obyvateli.
- V případě lepší fin. Gramotnosti může vznikat tlak na banky a vládní organizace, aby zlepšovaly své opatření v oblasti AML/CFT.

Technologické faktory:

- Rozvoj technologií jako jsou biometrická ověřování, umělá inteligence nebo blockchain.
- Kybernetická bezpečnost: lepší práce s veřejností ze strany NÚKIB.
- V oblasti AML/CFT je také důležitý neustálý vývoj v technologií – zavedení nových nástrojů a přístupů k identifikace podezřelých klientů a obchodů.
- Inovace – zlepšení kybernetické bezpečnosti, aby nebyla možnost zneužití nástrojů a celkového finančního systému.

5.2 Prevence proti AML/CFT ze strany Komerční banky za rok 2023

Komerční banka jako každý rok usilovně předchází zneužívání svých služeb před legalizací prostředků z trestné činnosti a financování terorismu. Slouží k tomu důkladné dodržování legislativních předpisů, norem jak ze strany regulatorních orgánů České republiky, tak také ze strany finanční skupiny Société Générale. V roce 2023 docházelo v oddělení Compliance k napravování a vylepšování interních procesů v reakci na externí audit od České národní banky.

Díky zavedenému systému pro monitoring veškerých transakcí je tak možné zlepšovat povědomí o průchodu transakcí, které mají spojitost s problematikou AML/CFT, jak z hlediska interních záchytů, tak také z hlediska korespondenčního bankovnictví. Korespondenční bankovnictví je forma bankovních operací, kde dochází ke spolupráci mezi více institucemi. V praxi je korespondenční bankovnictví nejčastěji využíváno prostřednictvím mezinárodních transakcí/plateb, kdy jedna banka využívá služby jiné

banky k uskutečnění převodu. Tato forma spolupráce napříč finančními institucemi po celém světě zlepšuje efektivitu a dostupnost bankovních služeb pro klienty a umožňuje plynulejší mezinárodní obchod včetně fungování finančních trhů jednotlivých zemí.

Rok 2023 byl pro celou finanční skupinu SG ovlivňován těmito událostmi:

- Ruská agrese vůči Ukrajině změnila procesy přijímání klientů do KB.
- Vytvoření a implementace detekčních nástrojů z pohledu AML sloužících k využívání i umělé inteligence, což má za cíl zefektivňování práce analytiků s informacemi o klientovi (propojenost nástrojů a jednotlivých oddělení). Každodenní využívání aplikace SIRON, která zachytává nestandartní/podezřelé transakce klientů pomáhá v boji proti praní špinavých peněz a terorismu.

5.3 Výsledky činnosti FATF za rok 2021 a 2022

Velikou příležitostí je bezpochybně digitální transformace celého světa. Digitalizace může velice pomoci v boji proti praní peněz a financování terorismu, nicméně každá z předností má také své zápory. Díky digitalizaci mohou být také veškeré subjekty (FO, PO) zranitelnější vůči podvodům a bezpečnosti.

Digitalizace má největší sílu v poskytování informací mezi jednotlivými stranami., můžeme mluvit o finančních institucích, mezivládních orgánech, aj. Důležitou změnou s prevencí proti praní peněz a financování terorismu je zjišťování původu majetku fyzických a právnických osob, včetně zaměření se na politicky exponované osoby. Důležitým bodem pro výbor FATF bylo také pašování migrantů a s tím byly spojeny značné finanční objemy transakcí, které podléhaly praní špinavých peněz. Po překonání globální krize způsobené Covidem -19 zasáhla svět okamžitě další krize v podobě ruské agrese na Ukrajinu. S touto agresí začaly vznikat otázky ohledně přílivu válečných migrantů.

5.4 Problematika AML/CFT zaměřená na postupy útvarů AML a AMLCOM

Součástí vyhodnocování podezřelých obchodů z hlediska praní špinavých peněz a financování terorismu jsou stanoveny obecné postupy a doporučení pro každého analytika, který pracuje v daném útvaru.

5.4.1 Analýza podezřelých alertů/transakcí útvarem AML

Tato kapitola praktické části diplomové práce obsahuje interní postupy analytického oddělení Compliance a útvaru AML a AMLCOM. V první části budou uvedeny reálné postupy při detekování a vyhodnocování nejen podezřelých obchodů, ale také postupy pro nepodezřelé alerty/transakce. Nejdříve je definována obecná analýza a náležitosti, které jsou v analýze obsaženy a poté také reálné postupy analytiků. Součástí kapitoly jsou také činnosti podléhající Compliance útvaru a tím je útvar AMLCOM. Tento tým analytiků má na starosti vyhodnocování alertů souvisejících s korespondenčním bankovnictvím. Jedná se o typ alertů, které jsou zachycovány aplikací AMLOCM skupiny SG. Korespondenční bankovnictví je forma bankovních operací, kde dochází ke spolupráci mezi více institucemi. V praxi je korespondenční bankovnictví nejčastěji využíváno prostřednictvím mezinárodních transakcí/plateb, kdy jedna banka využívá služby jiné banky k uskutečnění převodu. Tato forma spolupráce napříč finančními institucemi po celém světě zlepšuje efektivitu a dostupnost bankovních služeb pro klienty a umožňuje plynulejší mezinárodní obchod včetně fungování finančních trhů jednotlivých zemí.

Druhá část kapitoly bude zaměřena na výsledky útvarů AML a AMLCOM od roku 2019 do roku 2023 v porovnáním s trendem. Následná činnost oddělení Compliance bude komparována se statistikami Finančního analytického úřadu.

Analýza záchytů útvarem AML KB

Interní záchyty jsou v podobě alertů a jsou vyhodnocovány interními analytiky oddělení AML v aplikaci SIRON. Každý alert představuje potenciálně podezřelý obchod a obsahuje své ID. Je třeba alert prověřit, poté vyhodnotit a příslušným způsobem uzavřít. Při uzavření vyhodnoceného alertu je nutné vyjádření, které říká, zda byl obchod shledán

podezřelým či nikoli a uvedení informace ohledně dalších opatření. Alerty jsou zpracovávány dle priority, která závisí na různých faktorech a pořadí zpracování je dáno analytikem.

Faktory zohledňující přednostní zpracování:

- **kvantifikace rizika** – založeno na pravděpodobnosti, že daná transakce skutečně může být podezřelá a potenciálním dopadu na banku v případě detekování skutečně nezákonné transakce;
- **rizikovost klienta** – v případě podezřelé transakce, jehož součástí je rizikový klient označený statusem „MED-HIGH“ a „HIGH“
- **reputační riziko*** – negativní informace;
- **dle typu transakce** – neobvyklé transakce, transakce prováděné v hotovosti, objemovost transakce a mezinárodní transakce mířící do rizikových zemí (např. Afganistán, Sýrie, Jordánsko, aj.);

může se jednat také o klienty, kteří již v minulosti měli detekované „OPO“ nebo byli vyšetřováni státními orgány.

*Reputační riziko je takové riziko, které je spojeno s poškozením jména KB (přímo) a vznikem finančních ztrát (nepřímo), a které nelze přiřadit k riziku kreditnímu, finančnímu, operačnímu nebo likvidnímu. Mezi konkrétní reputační rizika patří:

- Přijetí subjektu do banky, který je spojen se závažnými negativními informacemi, její historické aktivity KB Group jsou spojovány s nelegální činností, která nebyla vysvětlena.
- Poskytnutí produktů/služeb KB osobám, které jsou spojeny s neetickými, nemorálními nebo nelegálními aktivitami, popř. klientům, které mají na takové osoby další přímé nebo nepřímé vazby.
- Realizace obchodů, které mohou vzbudit kritický zájem veřejnosti, médií (např. významné negativní sociální, ekologické nebo hospodářské dopady), popř. regulatorních a státních orgánů a institucí.

5.4.2 Přijetí interního záchytu potenciálních podezřelých obchodů:

Interní záchyt se týká opatření, která jsou implementována díky aplikacím uvnitř Komerční banky.

V rámci analýzy lze definovat několik úrovní vyhodnocování:

- **FALSE POSITIVE**: V případě, že AML analytik narazí na zjevně chybně vytvořený alert, uzavře ho jako nepodezřelý pod „False positive“ a stručně zdůvodní toto vyhodnocení.
- **PRIMARY ANALYSIS**: Pokud k vyhodnocení jako nepodezřelý je nutné základní analýza KYC, analýza transakcí, je analytikem uzavřeno jako „PRIMARY ANALYSIS“. Ve vyhodnocení je také nutné přidat krátkou poznámku se zhodnocením. V kompetenci analytika je možné požadování konkrétnějších informací, když se z dostupných informací nepodaří objasnit účel a povahu transakce. Daný sběr potřebných informací je zaslán na BaPo (bankovní poradce), analytik nikdy nekomunikuje napřímo s klientem.
- **CASE**: Pokud k vyhodnocení jako NEPODEZŘELÝ je zapotřebí hlubší analýzy KYC, transakcí a posouzení shody, uzavře ho AML analytik jako nepodezřelý s poznámkou CASE a zdůvodněním tohoto zhodnocení. Následně požádá Vedoucího Specialistu Compliance Analýzy transakcí o validaci rozhodnutí o uzavření alertu jako NEPODEZŘELÝ.
- **REPORTING**: Analytik stupně vyhodnotí předaný případ a rozhodne o podání hlášení o podezřelém obchodu na FAÚ.

Analýza potřebná k rozhodnutí obsahuje přiměřeně níže uvedené body

Postup analytika útvaru AML od úrovně „Primary analysis“:

Vyhledá veškeré relevantní informace k případu. Za tím účelem jsou využívány interní aplikace a informace na internetu (popř. listinné materiály žádá přímo po příslušném odpovědném zaměstnanci KB (bankovní poradce, pokladník, pracovník Back Office, aj.).

Mezi relevantní informace zpravidla patří:

- informace KYC oddělení;
- transakční historie (pohyby na účtu);
- vazby mezi klientem a dalšími subjekty v rámci banky.

Mezi prioritní alerty patří vždy případy, které vykazují známky:

- financování terorismu a praní špinavých peněz;
- klienti v šetření z důvodu již otevřeného jiného alertu, investigace z důvodu sankcí, aj.;
- PEP klienti.

Postup analytika útvaru AML od úrovně Case:

1) Zjistí, zda je klient již evidován v interní databázi (databáze s již vyhodnocenými podezřelými obchody) a přidělí případu nové číslo jednací. Je-li klient již z minulosti evidován, vyhledá předchozí případy, seznámí se s jejich historií a vyhodnotí změny, ke kterým došlo od posledního šetření/oznámení.

2) Provede celkovou analýzu případu, při které zohlední veškeré relevantní skutečnosti, např.:
   - rizikový profil klienta (a jeho statutárního orgánu, skutečného majitele) a zda je k těmto osobám známa nějaká negativní informace (např. již byly předmětem interního šetření, dotazu FAÚ, informací/spekulací v médiích apod.);
   - ověří, zda se nejedná o politicky exponovanou osobu;
   - vazba klienta a protistrany obchodu – zda je tato vazba transparentní (odpovídá realizovanému obchodu), je-li to možné zjistit rizikový a finanční/podnikatelský profil protistrany (s využitím vnitřních nebo veřejně dostupných zdrojů);
   - důvod a účel obchodu a zváží jeho ekonomické či jiné opodstatnění (smysluplnost);
   - soulad mezi oznámenou transakcí a dosavadní historií pohybů na účtu;

- původ majetku/finančních prostředků (posoudit vysvětlení klienta, jak bylo doloženo, zda existují pochybnosti, zda je původ odpovídající příjmovým možnostem klienta, aj.);
- okolnosti obchodu (např. klient doprovázen další osobou, nervozita klienta, nevěnování pozornosti vysokým poplatkům za služby, aj);
- veškeré „negativní" informace z veřejných zdrojů (např. podezřelé aktivity, podezřelé vazby mezi klientem a dalšími subjekty, aj.).

Nejedná se o vyčerpávající výčet, bohužel je nutné každý případ posuzovat individuálně s tím, že některé výše uvedené informace nemusí být relevantní, a naopak se mohou vyskytnout situace, které zde nejsou uvedeny a které je nutné individuálně posoudit. Každý z detekovaných alertů je jedinečný.

3) Rozhodne o oznámení/neoznámení podezřelého obchodu. V zásadě se nabízí následující varianty:
   - obchod bez podezřelé aktivity – další postup „nepodezřelý obchod";
   - obchod vykazuje znaky podezřelé aktivity = oznámení podezřelého obchodu – další postup viz „podezřelý obchod".

5.4.3 Nepodezřelý obchod

Pokud aktivity klienta nevykazují žádné znaky podezřelého obchodu a neexistují ani žádné jiné důvody pro další zpřísněný monitoring klienta, analytik útvaru AML postupuje následovně:

1) zjistí-li nedostatky, upozorní na ně bankovního poradce ve zpětné vazbě a vyžádá provedení okamžité nápravy;
2) alert vyhodnotí v aplikaci SIRON jako „nepodezřelý" a uzavře.

Pokud aktivity klienta nevykazují žádné konkrétní znaky podezřelého obchodu, avšak chování/transakce klienta jsou přesto nestandardní / neobvyklé / rizikové a je tedy přínosné další sledování aktivit klienta, iniciuje analytik útvaru AML dočasné nastavení zpřísněného monitoringu klienta.

V takovém případě analytik útvaru AML postupuje následovně:

1) zjistí-li nedostatky, upozorní na ně bankovního poradce ve zpětné vazbě a vyžádá provedení okamžité nápravy;
2) po odstranění všech nedostatků zjištěných v průběhu šetření doplní v aplikaci SIRON stručně důvody, proč obchod nebude oznámen na FAÚ;
3) alert vyhodnotí v aplikaci SIRON jako nepodezřelý a uzavře;
4) analytik uzavře případ a společně s podklady, o kterých rozhodne, že jsou pro případ relevantní, je uloží do příslušné složky kontrol.

5.4.4 Podezřelý obchod

Pokud analytik útvaru AML vyhodnotí interní hlášení podezřelého obchodu tak, že vykazuje znaky podezřelého obchodu ve smyslu AMLZ, zváží, zda hrozí nebezpečí zmaření nebo podstatného ztížení zajištění výnosu z trestné činnosti/financování terorismu.

Podezřelý obchod – odklad splnění platebního příkazu klienta

Obchod, u kterého je nutné zvážit odklad splnění platebního příkazu klienta o 24 hodin, má naprostou prioritu před jakoukoliv další aktivitou útvaru AML. Základní podmínkou pro odklad splnění platebního příkazu klienta (pozastavení obchodu o 24 hodin) je skutečnost, že finanční prostředky jsou dosud stále na účtu klienta, tzn. obchod nebyl dosud realizován. Primárně se jedná o výstupy z kontrol realizovaných před zadání platebního příkazu a dále tzv. manuálních hlášení příslušných odpovědných zaměstnanců KB.

Největší rizika zmaření nebo podstatného ztížení zajištění výnosů z trestné činnosti hrozí u následujících typů obchodů:

- transakce, které směřují do některé z tzv. vysoce rizikových a senzitivních zemí (viz. příloha č.3);
- finanční prostředky, jejímž zdrojem je transakce z vysoce rizikových a senzitivních zemí;

- hotovostní operace (výběry v hotovosti);
- finanční prostředky, které pochází z podvodného jednání (phishing, vishing, aj.).

Postup analytika útvaru AML následující:

1) Zajištění zadání blokace finančních prostředků – v případě blokace prostředků je nutné být důsledný, jelikož provedení blokace může mít vážné následky pro následné předání příslušným orgánům v trestním řízení.

2) Do systému, který je určený pro práci s klienty ze strany BaPo, je nutné vložení poznámky **„účet klienta omezen, probíhá šetření Compliance, tuto informaci nesdělovat klientovi**, která se zobrazí při každé práci s tímto klientem. V tomto případě nesmí bankovní poradce poskytovat žádné informace klientovy daného účtu.

3) Informuje příslušného bankovního poradce klienta (případně další odpovědné zaměstnance KB, kteří mohou mít vliv na realizaci příslušné pozastaveného obchodu) a poučí jej o povinnosti mlčenlivosti (případně dalších krocích, které budou pravděpodobně následovat). Zároveň poskytne bankovnímu poradci informace a podklady, které mohou být využity při následnou komunikaci s klientem, a informace o možném nebo předpokládaném dalším průběhu případu (zejména vymezení časové omezení účtu).

4) V případě jakýchkoli problémů s kontaktováním odpovědných zaměstnanců KB zajistí tuto komunikaci jiný pracovník útvaru AML, zatímco příslušný analytik útvaru AML přistoupí k okamžitému vypracování oznámení podezřelého obchodu na FAÚ.

5) Zpracuje a odešle oznámení podezřelého obchodu. Jeho součástí jsou vždy následující informace:
   - upozornění, že jde o odklad splnění příkazu klienta (pozastavení o 24 hodin);
   - v MoneyWeb aplikaci se zadá volba „NOVÉ HLÁŠENÍ 24“;
   - identifikační údaje subjektu, kterých se oznámení podezřelého obchodu týká;
   - základní údaje o účtu;
   - veškeré relevantní údaje o oznámeném obchodu (datum transakce, kdo ji inicioval, jaký sdělil účel transakce, původ finančních prostředků, podezření na nastrčenou osobu, aj.);
   - zdůvodnění, proč KB přistoupila k odkladu splnění příkazu klienta ve smyslu AMLZ, jaké jsou konkrétní znaky podezřelého obchodu;
   - relevantní podklady (např. výpisy, příkazy k úhradě, vkladové/výběrové pokladní doklady, avíza, doklady/ prohlášení o původu majetku, doklady doložené klientem během kontroly klienta, aj.) jsou-li dostupné bez zbytečných časových prodlev;
   - zaevidování případu do aplikace SIRON včetně příslušných informací a dokumentu pro FAÚ.

Podezřelý obchod – bez odkladu splnění příkazu

Pokud obchod klienta vykazuje znaky podezřelého obchodu a není možné/nutné/účelné provést odklad splnění příkazu klienta (transakce již byla provedena, nehrozí zmaření/podstatné ztížení zajištění výnosu z trestné činnosti), přistoupí analytik útvaru AML k jeho oznámení na FAÚ.

Postup analytika útvaru AML:

1) Zpracuje a odešle oznámení podezřelého obchodu. Jeho součástí jsou vždy následující údaje/informace:
   - identifikační údaje subjektu, kterých se oznámení podezřelého obchodu týká;
   - základní údaje o účtu;

- veškeré relevantní údaje o oznámeném obchodu (datum transakce, kdo ji inicioval, jaký sdělil účel transakce, původ finančních prostředků, podezření na nastrčenou osobu, aj.);
- zdůvodnění, proč KB přistoupila k odkladu splnění příkazu klienta ve smyslu AMLZ, jaké jsou konkrétní znaky podezřelého obchodu;
- relevantní podklady (např. výpisy, příkazy k úhradě, vkladové/výběrové pokladní doklady, avíza, doklady/ prohlášení o původu majetku, doklady doložené klientem během kontroly klienta, apod.) jsou-li dostupné bez zbytečných časových prodlev.

2) Po předání oznámení podezřelého obchodu na FAÚ analytik uloží příslušný soubor do aplikace SIRON
3) zařadí klienta do kategorie „rizikový klient“ s označením „MED-HIGH“,“HIGH“
4) Analytik útvaru AML uzavře složku společně s relevantními podklady.

5.5 Postupy pro vyhodnocení alertů v aplikaci AMLCOM

Aplikace SG generující na základě několika scénářů alerty s transakcemi v rámci korespondenčního bankovnictví.Veškeré zpracování alertů probíhá v KB interními analytiky a pro tuto aktivitu není outsourcing. Analytici veškeré aletry zpracovávají v rámci aplikace, zaznamenávají a vyhodnocují analýzy.

Tabulka 1 Scénáře aplikace AMLCOM

Scénář #	Hledisko	Definice
1	**Geografické**	Účelem je odhalit mezinárodní transakce s přihlédnutím k úrovni rizikovosti země odesílající finanční instituce, odesílatele platby a všech zprostředkovatelských bank zapojených do příchozí transakce.
2	**Geografické**	Cílem je odhalit mezinárodní transakce s přihlédnutím k rizikovosti země přijímající finanční instituce, příjemce transakce, zprostředkovatelských bank zapojených do odchozí transakce a zvýhodněné instituce.
3	**Geografické**	Pravidlo 3 má za cíl odhalit jednotlivé transakce procházející přes více vysoce rizikových zemí. Za tímto pravidlem se skrývá detekování zemí a protistran transakce.
5	**Chování klienta**	Pravidlo 5 odhaluje změny v chování klientů – počty transakcí za minulý měsíc vs. aktuální počty/objemovost transakcí/uvážení protistran obchodu (zda je příjemce stále stejný či se mění)
6	**Skryté vztahy**	Odhalení skrytých vztahů mezi protistranami – mezi jedním a více příjemci.
7	**Skryté vztahy**	Odhalení skrytých vztahů mezi protistranami – mezi příjemcem a více odesílateli.
8	**Exotické měny**	Cílem je detekování neobvyklých měn (mimo EURO, CZK, USD).
9	**Chování bank**	Pravidlo je nastaveno na chování a transakční historii bank – bez dlouhodobé aktivity.
10	**Struktura**	Pravidlo zaměřené na "rychlé" převody malých částek pod nastavenou prahovou hodnotou – malé částky směřující jednomu příjemci od několika odesílatelů.
11	**Struktura**	Pravidlo zaměřené na "rychlé" převody malých částek pod nastavenou prahovou hodnotou – malé částky směřující od jednoho odesílatele několika příjemcům.

Zdroj: vlastní zpracování na základě interních materiálu KB

Přednostní zpracování:

- dle měny se zpracovávají v následujícím pořadí –> USD, RUB, ..., EUR, CZK;
- vysoce rizikové země – tj. pravidla R1, R2, R3 + Lotyšsko, Litva, Estonsko, Spojené království, aj.

Výsledky analytické práce útvaru AMLCOM lze vyhodnocovat ve čtyřech formách:

1) **FALSE POSITIVE** – možnost vyhodnocení „false positive“ přichází v úvahu jen u alertů pod scénáři R1, R2 a R3, které se soustředí na rizikovost zemí. V případě, kdy ani jedna transkce v alertu nemá v přítomnosti zemi s rizikovostí „MED-HIGH“ nebo „HIGH“ je možno alert vyhodnotit tímto způsobem.

2) **LEGIT** – relevantnost alertu u kterého není spatřena podezřelé aktivita protistran. Lze dohledat potřebné údaje k vyhodnocení a není zde řádné podezření na AML/CFT.
3) **REQUEST** – v případě, že analytik potřebuje doložení relevantních dokumentů nebo doplňující informace o protistraně. Doplnění informací je zasíláno korespondenční bance prostřednictvím e-mailové komunikace nebo systému SWIFT (platforma pro mezibankovní komunikace s celém světě – převody transakcí a informativní činnost).
4) **ATYPICAL** – atypical jsou vyhodnoceny takové alerty, které obsahují podezřelé transakce. Uzavírány jsou tímto takové alerty u kterých nelze ani prostřednictvím „REQUEST" získat potřebně informace

5.5.1 Základní pravidla pro identifikace, kontrolu a dotazování

Právnická osoba

U každé právnické osoby je potřeba identifikovat předmět činnosti. V případě, kdy tyto informace nejsou dostupné z veřejných zdrojů nebo interních zdrojů a transakce se jeví jako nestandardní, je nutné zaslat požadavek „REGUEST". V případě získání informací z veřejných zdrojů je nutné veškeré relevantní informace doložit k vyhodnocení alertu/transakce.

Fyzická osoba

V případě detekování potenciální protistrany na PEP s opakujícími se transakcemi nad limit 1.000 EUR je z pohledu analytika nutnost na identifikaci od banky vystupujících protistran. Když je jedna z protistran vyhodnocena jako PEP je nutné doložit údaje o původu finančních prostředků a zjistit účel transakce. Každá fyzická osoba je prověřována v mezinárodních rejstřících „Worldcheck", kde jsou uvedeny trestné činy nebo negativní informace.

5.5.2 Příklad oznámení podezřelého obchodu na Finanční analytický úřad

Jako korespondenční banka jsme zachytily transakci ve výši 390 000 EUR směřující od fyzické osoby Dorley Tamathy vlastníka Dorley Yachts (Monako) (MC5830003015040002061411174) do slovinské společnosti SLO Yachts (SLO8833000000002945032111), která je vedena Janou Jaakobovičovou. Účelem transakce měl být prodej luxusní jachty Alladin.

Transakce se nám jeví riziková zejména z důvodu pochybnosti slovinské společnosti. Společnost SLO YACHTS evidentně prodávající luxusní jachty, avšak nedisponuje internetovými stránky a jediné informace lze získat ze slovinského rejstříku ajpes.eu.
O odesílateli jsme získali osobní informace včetně čísla pasu, smlouva o prodeji nebyla dodána. Také jsme v rámci SWIFTu kontaktovali slovinskou banku SID bank, d.o.o, nicméně od této banky jsme i přes urgence žádnou odpověď nedostali.

Pochybností této transakce je i fakt, že pro Dorley Yachts prodává luxusní jachty manžel majitelky SLO Yachts, který ve společnosti vůbec nefiguruje. Na stránkách startitup.slo je uvedeno, že Ivan Jaakobovič prodal luxusní jachtu také ruskému oligarchovi.

V rámci oznámení na FAÚ je nutné doložit také veškeré zjištěné informace (výpisy, příkazy k úhradě, vkladové/výběrové pokladní doklady, avíza, doklady/ prohlášení o původu majetku, doklady doložené klientem během kontroly klienta) včetně webových odkazů. Oznámení je předáno na FAÚ v rámci aplikace MoneyWeb.

5.6 Analýza a zpracování dat z aplikací SIRON a AMLCOM

V této kapitole jsou analyzována a pracována data, která jsou poskytnuta z Komerční banky, a.s. Zpracována jsou data, která jsou výstupem procesů vyhodnocování podezřelých obchodů z aplikací SIRON a AMLCOM.

5.6.1 Analýza a zpracování dat z aplikací SIRON

Tabulka 2 Výstup z aplikace SIRON

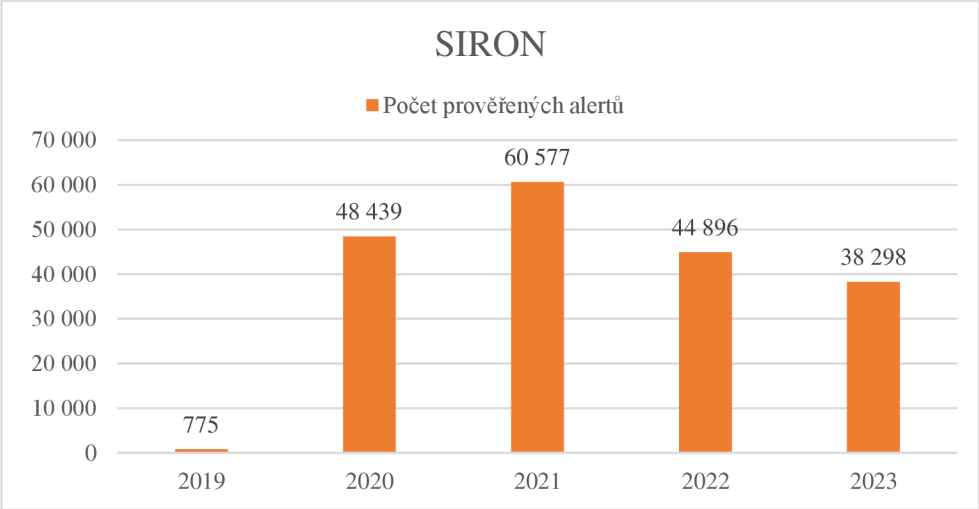
SIRON	2019	2020	2021	2022	2023
Počet prověřených alertů	775	48 439	60 577	44 896	38 298
Počet podezřelých transakncí na FAÚ	248	444	593	627	615
Platby vyřazené ke specialnímu monitoringu kvůli AML/CFT	X	X	1 549	4 353	8 544

Zdroj: vlastní zpracováni na základě výročních zpráv KB

V tabulce níže je zobrazena činnost útvaru AML, který má na starosti detekování a vyhodnocování podezřelých obchodů z aplikace SIRON. Data jsou znázorněna od roku 2019 do roku 2023. V boji proti AML/CFT v Komerční bance má největší zastoupení oddělení AML s využíváním aplikace SIRON. Jedná se o stěžejní aplikace pro boj a prevenci AML/CFT.

Graf 1 níže znázorňuje, jak v roce 2020 nastal enormní nárůst v v rámci prověřených alertů (48.439), což je následkem změny procesů ve schvalování, přijímání nových klientů a tím také nárůstu klientských a monitorovaných transakcí. Nárůst roku 2021 je dle výroční zprávy za rok 2021 zapříčiněn implementací zlepšených procesů k detekci podezřelých transakcí. Roku 2022 nastal celkem značný pokles v počtu prověřených alertů díky revizi procesů a scnénářů, kterými se detekují podezřelé alerty a nastala také optimalizace prahových hodnot. V tomto roce je možné také registrovat začátek ruské agrese na Ukrajinu a také fakt, že se Komerční banka zavázala ke značným výplatám klientů ruské banky Sberbank v ČR.

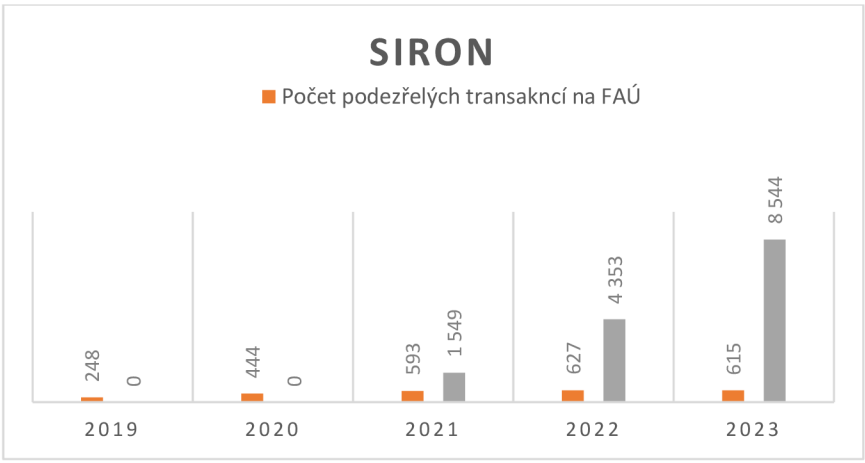
Graf 1 Počet prověřených alertů SIRON



Zdroj: vlastní zpracováni dle tabulky 2

Graf níže znázorňuje počty předaných transakcí na Finanční analytický úřad ze strany útvaru AML. Od roku 2019 do roku 2021 je značný nárůst, kdy rozdíl mezi rokem 2019 a 2021 je 345 transakcí podaných k prověření ze strany FAÚ. Od roku 2021 do roku 2023 není rozdíl tak relevantní. Naopak největším nárůstem od roku 2021 do roku 2023 jsou počty plateb vyřazených ke speciálnímu monitoringu kvůli AML/CFT. Jedná se o hloubkovou kontrolu občanů a klientů banky KB z Blízkého východu a jiných rizikových zemí.

Graf 2 Počet podezřelých transakcí



Zdroj: vlastní zpracováni dle tabulky č.2

5.6.2 Analýza a zpracování dat z aplikací SIRON

V tabulce níže je zobrazena činnost útvaru AMLCOM, který má na starosti detekování a vyhodnocování podezřelých obchodů ze strany korespondenčního bankovnictví. Data jsou znázorněna od roku 2020, kdy byla aplikace AMLCOM spuštěna.

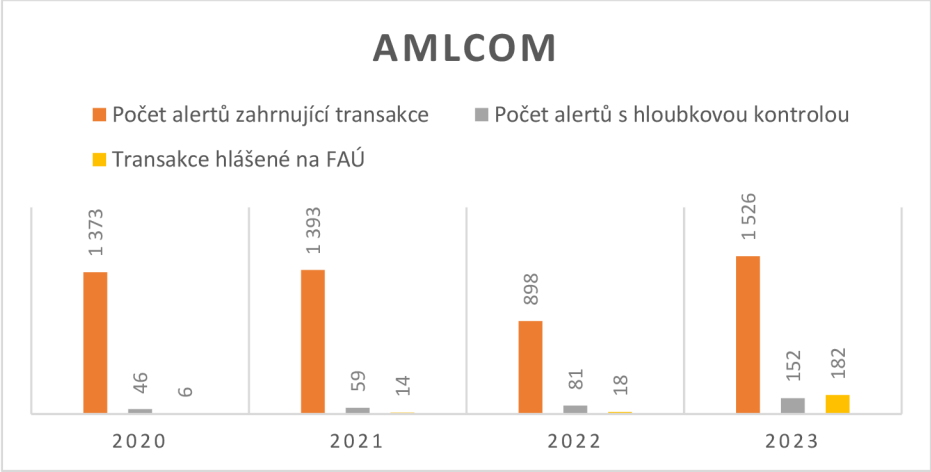
Tabulka 3 Výstup z aplikace AMLCOM

AMLCOM	2020	2021	2022	2023
Počet alertů zahrnující transakce	1 373	1 393	898	1 526
Počet alertů s hloubkovou kontrolou	46	59	81	152
Transakce hlášené na FAÚ	6	14	18	182

Zdroj: vlastní zpracováni na základě výročních zpráv KB

Díky vývoji technologií s využitím umělé inteligence je práce analytiků efektivnější a jak je vidět na grafu níže, tak i statistiky mluví za vše. Díky analýze korespondenčního bankovnictví se každoročně zvyšovaly statistiky, včetně hlášených transakcí na FAÚ (graf 3), kdy v roce 2023 bylo nahlášeno ze strany AMLCOM 182 transakcí ze 152 hloubkově prověřených alertů.

Graf 3 Graf s počty alertů a transakcí hlášenými na FAÚ



Zdroj: vlastní zpracováni dle tabulky 3

5.7 Činnost Finančního analytického úřadu

V tabulce 5 jsou vyhodnoceny statistiky Finančního analytického úřadu v období od 2017 do 2022.

Tabulka 4 Statistiky finančního analytického úřadu

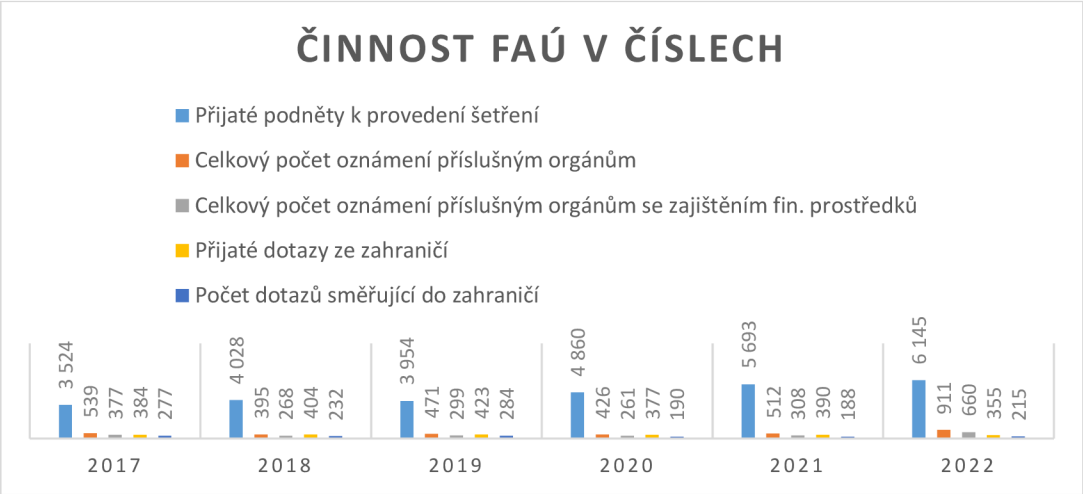
Finanční analytický úřad	2017	2018	2019	2020	2021	2022
Přijaté podněty k provedení šetření	3 524	4 028	3 954	4 860	5 693	6 145
Celkový počet oznámení příslušným orgánům	539	395	471	426	512	911
Celkový počet oznámení příslušným orgánům se zajištěním fin. prostředků	377	268	299	261	308	660
Přijaté dotazy ze zahraničí	384	404	423	377	390	355
Počet dotazů směřující do zahraničí	277	232	284	190	188	215
Výše zachráněných finančních prostředků (v mil. Kč)	2 146	7 546	2 269	3 897	2 027	2 606
Udělené pokuty pro porušení AMLZ (v mil. Kč)	2 490	2 114	1 950	2 695	4 120	6 865

Zdroj: vlastní zpracováni na základě výročních zpráv FAÚ

Graf 4 popisuje informace o činnosti Finančního analytického úřadu v rámci boe proti praní špinavých peněz a financování terorismu v průběhu let 2017 – 2022. Popisovány jsou za autora nejdůležitější statistiky v tomto období v rámci problematiky AML/FCT. Od roku 2017 je možno v grafu vidět každoroční nárůst veškerých statistik související s prevencí a bojem proti AML/CFT. Tyto změny jsou zapříčiněny změna a trendem v oblasti boje proti AML/CFT v globální úrovni. Faktory, které ovliňujíc změny a trendy jsou především ve vývoji technologie , změn regulačních opatření. Nakonci roku 2019 a začátku roku 2020 do celého světa přišla pandemie Covid-19, která zapříčinila okamžitou digitalizace v rámci všech odvětví, v boji proti praní peněz a financování terorismu tomu nebylo jinak. Nejdůležitějšími ukazateli v činnosti FAÚ jsou bezpochyby přijaté podněty k prověření. Za pravidelným nárůstem je posílení právě již zmiňovaného boje proti praní peněz včetně prevence.

OD roku 2017 do konce roku 2022 je možno vidět skoro 2x růst prověřených podnětů ze strany FAÚ. V rámci činnosti FAÚ se zvyšují nejen počty oznámení podnětů, ale také i podněty, které jsou považovány trestným činem.

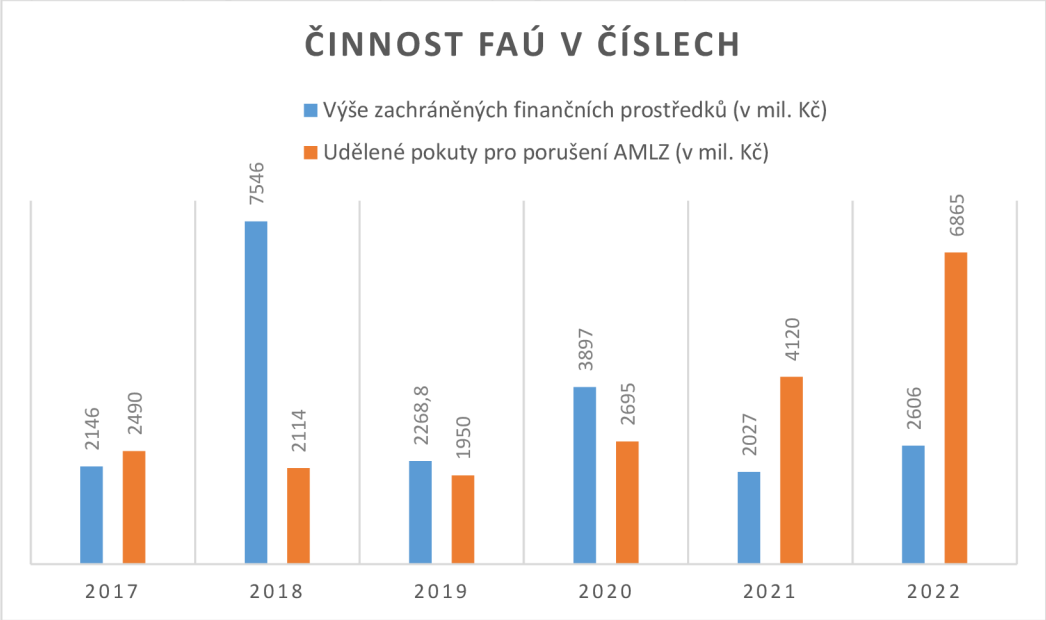
Graf 4 Činnost FAÚ



Zdroj: vlastní zpracováni dle tabulky 4

V grafu níže jsou znázorněné statistiky ze dvou pohledů, kde první znázorňuje výši zachráněných prostředků v milionech Kč, zatímco druhý znázoňuje výši udělení pokut pro porušení AMLZ v milionech Kč. Především ukazatel udělených pokut dostál značných nárůstu a je zjevné, že je to díky zvyšujícím se nárokům na boj proti dané problematice AML/CFT. Udělené pokuty za rok 2022 se dostali do rekordní výše 6,865 mil. Kč. Z pohledu statistik výše zachráněných prostředků dominuje rok 2018, kdy v roce 2018 je rekordní záchrana 7,546 mil. Kč. Tato částka představuje reakci na změny v boji proti AML/CFT ze strany ČR a také EU.

Graf 5 Výše zachráněných prostředků a výše udělených pokut ze strany FAÚ



Zdroj: vlastní zpracováni dle tabulky 5

5.8 Platební podvody

Platební podvody jsou druhou kapitolou praktické části diplomové práce. Platební podvody jsou trestným činem z oblasti kybernetické kriminality, a v dobách pokročilé digitalizace také velmi častým jevem. Od začátku pandemie Covid-19 na přelomu roku 2019 a 2020 byla požadována větší digitalizace všech odvětví a také celé bankovní sféry. Klienti bank měli zájem o uživatelsky příjemnější komunikaci s bankou a správu svých bankovních služeb. Banka se snaží předcházet těmto trestným činům v podobě aktivní a pasivní ochrany svých klientů.

5.8.1 Aktivní ochrana

Banka se samozřejmě snaží všemi možnými způsoby podvodníkům překazit přístup do aplikací banky, a tím pádem na účty klientů (např. bankID – založení dalších „podvodných“ účtů v JPÚ). Nejčastěji klienti předávají své přihlašovací údaje, čísla karet a ověřovací metody (Kb klíč, login a heslo z SMS) pomocí podvodných phishingových stránek či vishingových hovorů, nebo v rámci podvodných investic. Klienti dávají podvodníkům dobrovolně volný přístup do svých bankových aplikací a v krajních případech jim přenechávají volné využíváni svých účtů.

Dříve Komerční banka využívala v rámci aktivní ochrany takzvaný „cronto kód“ (obrázek 12), který se zobrazoval klientovi vždy, když se snažil přihlásit do internetového bankovnictví z nového zařízení (ať už tablet či počítač). Sloužil jako poslední míra obrany a zadržení klienta, že „dělá něco, co by neměl“. Princip byl jednoduchý – pokud se klient (nebo útočník) hlásí přihlašovacími údaji klienta z nového zařízení, které předtím klient nepoužil, pak se zobrazí před přihlášením do IB tento barevný kód. Klient musí tento kód aktivně naskenovat foťákem ve svém telefonu, při aktivní aplikaci KB klíče (vidina byla, že klient musí být přihlášení přítomen tak, aby mohl vzít telefon, ten odemknout a potvrdit naskenováním pomocí KB klíče tento obrázek a následně potvrdit notifikaci otiskem prstu). Součástí notifikace v KB klíči je i varování, že klient potvrzuje přihlášení ze zcela nového zařízení a zda si přeje opravdu toto zařízení potvrdit.

Obrázek 12 „Cronto kód“

Zdroj: interní materiál KB, 2023

Bohužel, podvodníci pochopili největší slabinu tohoto opatření a to, že stačí zcela jednoduše klienta přesvědčit, že mají jen zájem o nákup zboží (bazarový podvod) a k tomu, aby klient zboží „prodal“, musí ve svém bankovnictví potvrdit příjem financí. K tomu podvodník poskytl i phishingovou stránku s podvodným přihlášením, kdy v rámci komunikace podvodníci taktéž z originálních stránek KB (kam vyplnili získané klientovy přihlašovací údaje) poslali výřez „cronto kódu“ klientovi. Ten si obrázek stáhl do dalšího zařízení, naskenoval KB klíčem a potvrdil přihlášení z nového zařízení, a tím dal kompletní přístup podvodníkovi do svého bankovnictví. Zde banka následně přikročila

k co největšímu zkrácení doby platnosti toho kódu (při spuštění byla doba platnosti 10 minut, což se ukázalo jako moc dlouhá doba), která se ustálila na zhruba minutě času platnosti. Díky tomuto času již podvodníkovi znemožnila tento proces uskutečňovat.

Týmy platebních podvodů Komerční banky se pouze s „cronto kódem“ nesmířily, ale požadovaly komplexnější a kvalitnější ochranu. Banka následně na to přišla se zavedením tzv. animovaného QR kódu (frekvenční animace a změny). Tento QR kód, plně „cronto kód“, se stal prozatím nejúspěšnějším opatřením, které bylo proti phishingu implementováno. Pro podvodníky je velice složité či přímo nemožné replikovat animaci a předat ji klientovi, aby ji svým Kb klíčem naskenoval v reálném čase, a tím potvrdil přístup do bankovnictví. Jednotlivé sekvence obrázků mají velice krátkou životnost (cca půl sekundy) a zobrazení je možné pouze jednou. Podvodník tedy nemá jak tyto animace klientovi předat k verifikaci. Toto opatření vedlo k veliké eliminaci formy phishingu jako takového.

5.8.2 Pasivní ochrana

Pasivní ochrana je ochrana ze strany klientů KB proti případným platebním útokům. Jedná se o soubor doporučení a pravidel, která jsou bankou doporučována k udržování prevence před útoky. Komerční banka uvádí „desatero bezpečnosti“, skládající se z deseti opatření a zásad, které jsou potřeba ze strany klientů dodržovat, aby byli na internetu dostatečně ochráněni. V rámci těchto zásad je nejdůležitější zejména navštěvovat pouze známé webové stránky (v případě přístupu do aplikací Kb pouze přes oficiální stránky), používat bezpečná a silná hesla, neotevírat podezřelé komunikace a dbát na ochranu svých údajů.

V případě ochrany zařízení je důležité disponovat antivirovým programem, který odhalí obsah škodlivých dat. K přihlašování do internetového bankovnictví pro správu bankovního účtu je nutné se přihlašovat z bezpečných zařízení. Klienti se musí vyvarovat přihlašování z kaváren nebo z veřejně dostupných internetových připojení. Právě veřejná internetová připojení jsou nejvíce využívána ze stran podvodníků. Mobilní bankovnictví je chráněno ze strany banky, ale mobilní telefon si klient již musí ochránit sám. Účinnou ochranou je kvalitní zabezpečení pomocí silného hesla, otisku prstu, FaceID nebo nainstalováním malwaru, který představuje ochranu před škodlivými aplikacemi.

Nejzranitelnější pro klienty bank jsou platební karty a platby na internetu. Doporučenou ochranou a nejúčinnější je ochrana PIN kódu. PIN kód by neměl obsahovat jednoduše rozpoznatelné spojení číslic (1234,1111, aj.) a v případě, kdy je platební karta používána v bankomatu, je vhodné si zadávání PIN kódu chránit tělem. Důležitou ochranou je také být obezřetný v přítomnosti bankomatu, v současné době jsou na bankomatech instalovány systémy, které snímají údaje karty. Vhodnou ochranou je přikládání karet bezkontaktní formou, jak při placení telefonem (hodinkami) v obchodě.

Obrázek 13 Podvodný snímací systém karet

Zdroj: iROZHLAS,2013

5.8.3 Systém FDS (Fraud detection system)

Každá banka má svůj vlastní FDS systém. Ten funguje na principu tzv. scoringu plateb. Tedy každá zadaná (ať už tuzemská či zahraniční) platba dostane vyhodnocením svoji hodnotu. Systém pak podle hodnoty, která buď překročí či nepřekročí nastavenou mez (pro pozastavení platby) provede předem určenou akci v rámci pravidel. Akce jsou různé

– např. pozastavení platby, zamítnutí platby (platba na sankcionovanou osobu /účet/zemi/banku), zpracování platby, aj. Skórovány jsou veškeré, ať už platební, či karetní transakce klienta. Systém umožňuje taktéž skórovat i např. biometrickou stopu klienta (pohyb po obrazovce, rytmus stisku kláves, otisky prsů, obličej, hlas…), či další

komponenty jako například aktivní hovor v telefonu při zadání transakce skrze mobilní banku, nové zařízení, založení účtu přes bankovní identitu apod.

Každý takový systém využívá sadu pravidel, možnosti biometriky, scénáře (zjednodušeně – pokud klient udělá určitou akci, tak systém na danou akci zareaguje). Nejčastěji předem zadaná pravidla systému pomáhají nejvíce při zachycování podezřelých plateb. Jedny z nejčastějších, které lze uvést, jsou například – nové zařízení klienta, nová IP adresa pro přístup do bankovnictví, netypicky velká transakce, transakce do zahraničí apod. Samozřejmostí je i využití tzv. „Watchlistů". Watchlisty mohou být úzce specifické (například na známé číslo sankcionované osoby, nebo číslo účtu specifického podvodníka které jsme zjistili), na zemi, banky, ale i určité obchodníky či našeho klienta (je-li potřeba monitorovat jeho platby). Nejčastější varianta watchlistů je ale na podvodného příjemce – tedy banka zjistila v rámci preventivního ověřování, že dané číslo účtu směřuje na podvodníka v rámci typických podvodných scénářů. Povinností banky je před takovýmito platbami, které mohou vyústit ve ztrátu finančních prostředků, vždy klienta varovat.

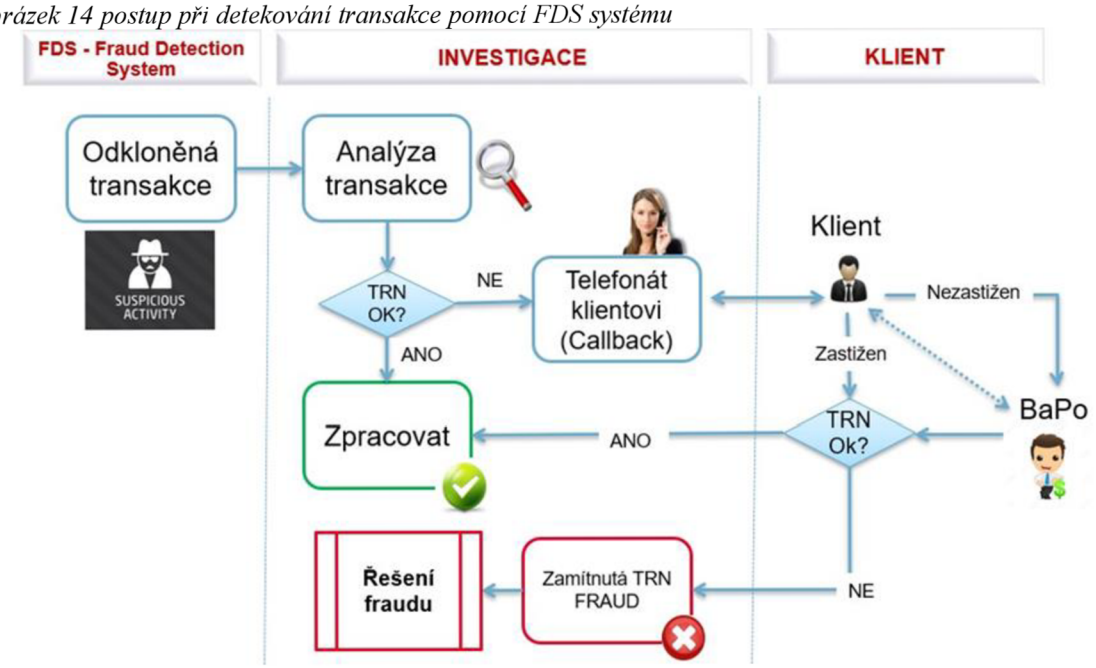
V FDS systému pro platební transakce v KB (skrze internetovou a mobilní banku) proběhne a je zkontrolováno cca půl milionu transakcí denně. FDS systém je zpracovává a oddělení prevence platebních podvodů prověřuje transakce, které systém vyhodnotil jako podezřelé. Běžně se jedná o analýzu cca 200-300 transakcí denně, z nichž je v průměru 5-10 podvodných. Tyto transakce souvisí s podvody, vedou na podvodná čísla účtů anebo jsou jinak podezřelé a hrozí ztráta finančních prostředků klienta.

Na obrázku níže () je znázorněn postup při podezřelé transakci vyhodnocené FDS systémem. Transakce, která je vyhodnocena jako podezřelá tzn. vysoká „skoring", je prostřednictvím systému předána na oddělení platebních podvodů, kde následuje hloubková analýza transakce analytikem. Vyhodnocení je možno provést dvěma způsoby. Prvním způsobem je skutečnost, kdy analytik neshledá transakci podezřelou, a tím dovolí platebnímu systému platbu zpracovat.

V případě druhého způsobu, kdy analytik shledá transakci podezřelou, následuje oznamování klientovi. V případě, že je klient zastižen, probíhá komunikace ohledně podezřelé transakce. Pokud je klientem vysvětlena a potvrzena jako nepodezřelá, je pustěna platebním systémem ke zpracování. Druhou možností je nevědomost o transakci

ze strany klienta, tím pádem je transakce vyhodnocena jako podezřelá a přebírá ji odpovědný analytik k řešení. Avšak pokud není klient zastižen, následuje informování BaPo a předání pokynů k řešení.

Obrázek 14 postup při detekování transakce pomocí FDS systému



Zdroj: interní materiál KB, 2024

Platby na internetu jsou snad nevíce rizikovou oblastí, jak přijít o finanční prostředky. Ze strany Komerční banky jsou veškeré platby na internetu monitorovány a pomocí systému FDS zabezpečeny.

Systém FDS:

- prověří 500.000 transakcí denně;
- prověřuje platby na internetu a přiřazuje „scoring“ platby;
- zachránil 384 milionů Kč;
- detekoval více než 2.330 podvodů.

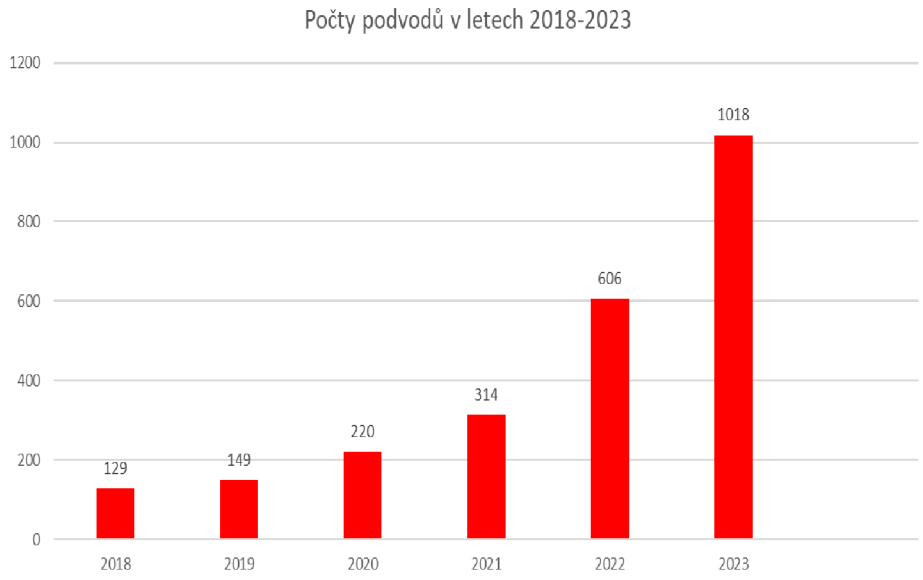
Obrázek 15 Čísla FDS systému

Zdroj: Komerční banka, a.s., 2024

Největší příčinou nárůstu v počtu podvodů je globální pandemie Covid-19. Jak již bylo zmíněno, Covid-19 započal extrémní digitalizaci ve všech sférách a spousta věcí tomu byla přizpůsobena. Jelikož se ale jednalo o novou věc, některé věci se také zjednodušily. Tato skutečnost přítomnosti Covidu a digitalizace nahrála podvodům ve velké míře. Grafy níže jsou statistikami Komerční banky pouze v oblasti platebních podvodů a znázorňují enormní vývoj v počtech detekovaných podvodů.

Graf 6 znázorňuje celkový počet zachráněných podvodů za období 2018-2023, a to pouze skrze internetové a mobilní bankovnictví. Od roku 2019 je nárůst téměř o 600 %. Rok 2023 přinesl zachycení 2.333 podvodů, přičemž zachráněných transakcí bylo 1018.

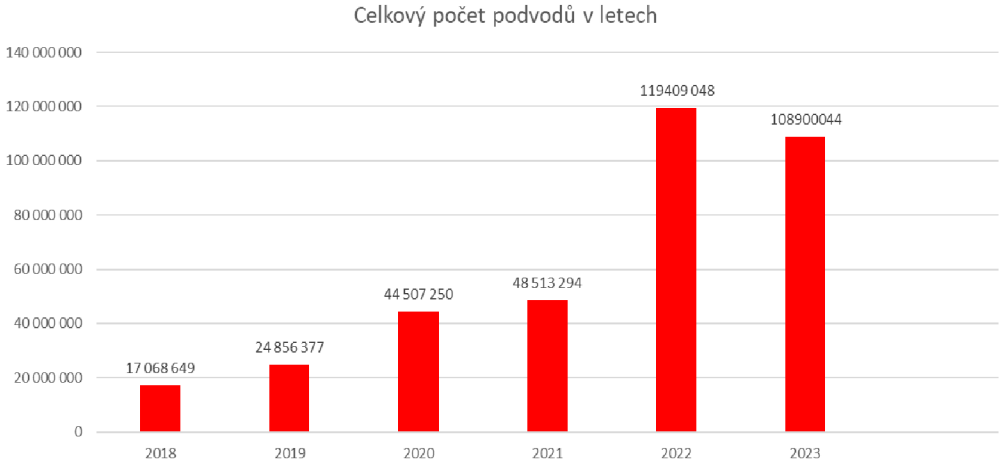
Graf 6 Počty podvodů v letech 2018-2023



Zdroj: výstup FDS systému

Graf 7 ukazuje zachráněnou částku z hlediska platebních podvodů za období 2018 až 2023. Za rok 2023 bylo zachráněno Komerční bankou více než 108 milionů Kč. Celková částka, o kterou byli klienti připraveni, dosahuje téměř 380 milionů Kč. Největším záchytem z pohledu analytiků byla částka 13 milionů Kč.

Graf 7 Celkový počet podvodů v období 2018-2023

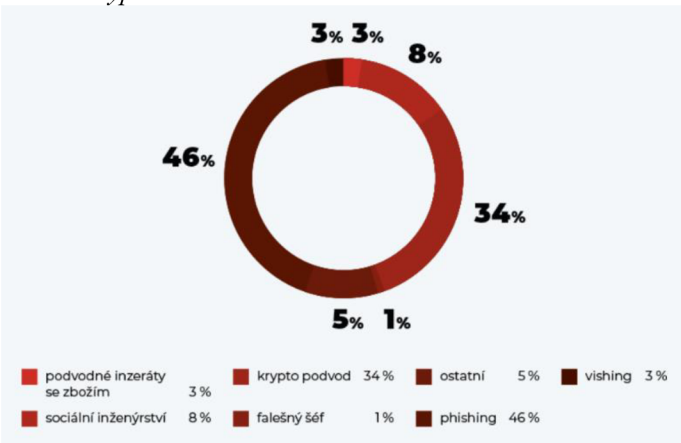


Zdroj: výstup FDS systému

Graf 8 podílu podvodů podle typu za rok 2022 zobrazuje procentuální zastoupení jednotlivých typů platebních podvodů na základě celkového počtu v daném roce. Tento graf poskytuje informace o relativním významu jednotlivých typů podvodů v rámci celé problematiky platebních podvodů.

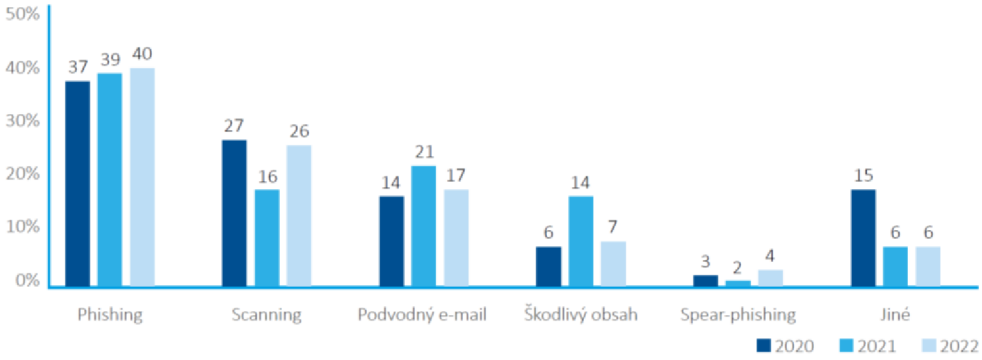
Podíl podvodů dle typu v Komerční bance za rok 2022 nepřinesl oproti minulým obdobím změny. Stále největší podíl na platebních podvodech mají typy phishingového podvodu a krypto podvodu. Phising se podílel 46 % na veškerých podvodech a krypro podvod 34 %. Národní úřad pro kybernetickou a informační bezpečnost vykazuje data s nejčastějšími platebními podvody v rámci celé České republiky. Na základě těchto dat je tedy zřejmé, že statistika platebních podvodů v KB je shodná s trendem v celé České republice. Za rok 2022 NÚKIB uvádí, že phishingový útok má 40 % podíl (graf 9) na veškerých podvodech v rámci internetové sítě. Z hlediska statistik dále NÚKIB uvádí, že celých 92 % respondentů ČR se setkalo s potenciálních phishingovým útokem.

Graf 8 Graf podílu podvodů dle typu za rok 2022



Zdroj: KB, 2024

Graf 9 Podíl podvodů dle typu u respondentů NÚKIB za rok 2022

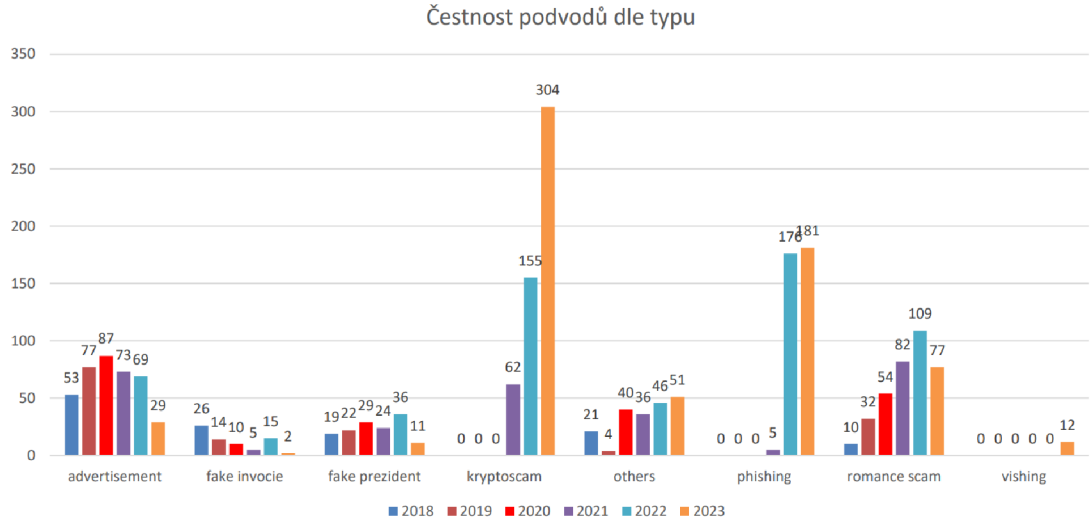


Zdroj: NÚKIB, 2023

Graf 10 četnosti podvodů dle typu zobrazuje absolutní počet podvodů pro každý typ podvodu bez ohledu na celkový počet v jednotlivém roce, bez ohledu na celkový počet podvodů v daném období. Graf v období za rok 2023 ukazuje 304 případů krypto podvodu, které byly detekovány. Tento graf poskytuje informaci o tom, které typy podvodů jsou nejběžnější.

Následující analýza bude provedena z dat Komerční banky o rozsahu a charakteru platebních podvodů. Celkový počet podvodů jen ze stran klientů Komerční banky je alarmující. Četnost podvodů dle typu poskytuje důležitý pohled na to, jaké metody jsou nejčastěji ze stran podvodníků využívány. Na grafu níže je vidět četnost podvodů dle typu, které jsou nejvíce rozšířené u klientů Komerční banky.

Graf 10 Četnost podvodů dle typu

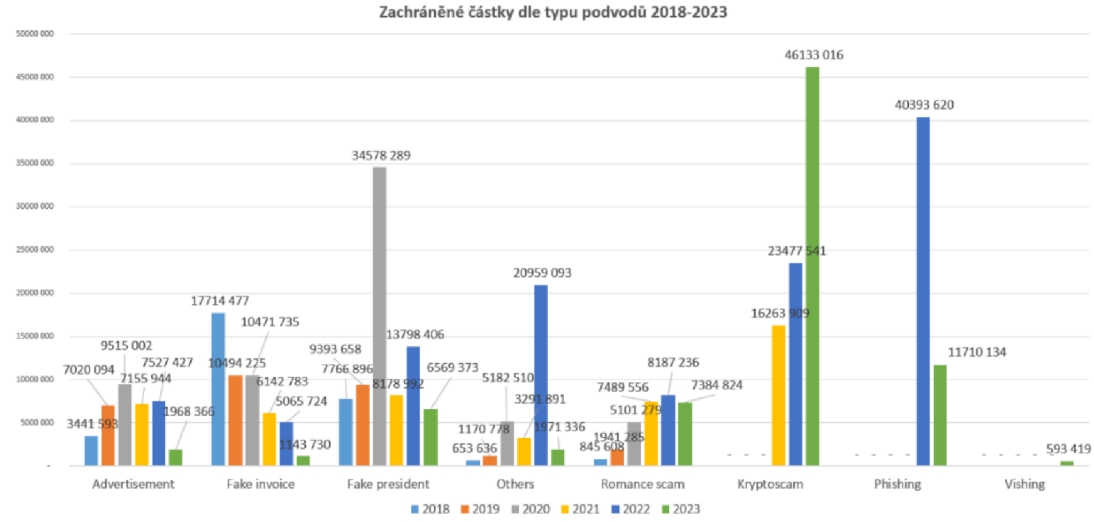


Zdroj: výstup FDS systému

Rozdíl mezi grafy procentuálního podílu a četností podvodů dle typu spočívá v tom, jak jsou data intepretována. Záleží na tom, zda jsou data zaměřena na procentuální zastoupení nebo na absolutní četnost jednotlivých typů podvodů.

Graf o zachráněných částkách dle typu podvodů v období 2018-2023 poskytuje důležitý pohled na úspěšnost opatření v boji proti platebním podvodům ze strany Komerční banky. Uvedené částky u jednotlivýh příkladů zobrazují, kolik finančních prostředků bylo díky odhalení systému FDS a anylitikům zachráněno v průběhu těchto let.

Graf 11 Zachráněné částky dle typu podvodu 2018-2023



Zdroj: výstup FDS systému

V případě analýzy daný graf (11) poskytuje několik klíčových poznatků. Nejen, že představuje vývoj nových typů podvodů ze stran podvodníků, ale také účinnost opatření. Díky rostoucím částkám, které jsou zachráněny z pohledu vývoje je patrné, že nastavená opatření ze strany Komerčná banky fungují. Samotná čísla u phishingových/krypto/fake president podvodů mluví za vše. Lze říci, že nastavená opatření v boji proti platebím podvodům jsou účinná a správná.

Věková kategorie obětí platebních podvodů klientů Komerční banky je důležitým faktorem. Vypovídá o tom, která věková kategorie je nejvíce ohrožena. Dle dat Komerční banky je nejvyšší četnost podvodů cílena na střední věkovou kategorii. Důvodů může být uváděno několik, nicméně nejzásadnější důvod, proč je cíleno na tuto kategorii je, že občané v tomto věku jsou ekonomicky velice aktivní a mají větší finanční stabilitu než ostatní. Jedná se také o počty prováděných převodů a o zvýšenou činnost v internetovém a mobilním bankovnictví. Mezi další důvod je možné zařadit rozvod. Rozvodovost občanů ČR je nejvyšší ve střední věkové kategorii a díky tomu spousta klientů disponuje větším počtem finančních prostředků (vyrovnání společného jmění manželů).

Graf 12 Četnost věkových kategorií

Zdroj: výstup FDS systému

7 Výsledky

Kapitola bude seznamovat s výsledky a vlastními poznatky autora diplomové práce. Na základě analýz provedené s pomocí dat z interních aplikací SIRON a AMLCOM je možno vyhodnotit pozitivní trend nastolených praktikách a procesech proti praní špinavých peněz a financování terorismu. Na základě interních postupů jsou zjištěny výsledky za období před pandemií Covid-19, včetně ruské agrese na Ukrajinu. Jak je již zřejmé z výsledků této praktické části je zřejmé, za právě tyto dvě globální události mají vliv na celý svět. Veškeré tyto krize dávají prostor pro nárůst a šíření podvodů a nelegálních aktivit. Nicméně je vidět z výsledků analýz, že i když je nárůst nelegálních praktik, tak procesy ze stran regulatorních orgánů jsou nastaveny velice dobře. Není tím myšleno jen ze strany mezinárodních organizací jako je FATF, ale také i ze strany Evropské unie a České republiky. V České republice na tom mají největší zásluhu orgány v podobě České národní banky a Finančního analytické úřadu. Ve srovnání dat z roku 2018 a 2022 je vidět, že jen Finanční analytický úřad registroval dvakrát více oznámení o podezřelých obchodech. Celkově práce poskytuje detailní pohled na strategie a opatření Komerční banky v boji proti finančním zločinům a zdůrazňuje vliv globálních událostí.

Zabezpečení bank a ochrana klientů před platebními podvody jsou neustále se vyvíjející oblastí, která vyžaduje trvalou pozornost ze strany bank. Vzhledem k tomu, že podvodníci neustále přicházejí s novými metodami je nutné taky zaměřovat svou činnost na inovace v oblasti zabezpečování. S nárůstem digitálních technologií se zvyšuje riziko i podvodů, čemuž výsledky jasně odpovídají. Od roku 2019 nastal enormní nárůst veškerých forem podvodů a o až o 600 %. Banky jakožto klíčový subjekt v tomto ohledu se již aktivně angažuje v boji a prevenci s těmito podvody, díky implementace interních FDS systémů může reagovat na veškeré změny a být díky tomuto systému velice efektivní v záchraně finančních prostředků klientů. Díky spolupráci veškerých finančních subjektů se a neustálým procesem inovací relativně dobře daří bojovat jak už v praním špinavých peněz, tak i s detekování platebních podvodů.

Jelikož nejvíce podvedenou věkovou kategorií jsou občané ve středním věku účinnou zbraní pro prevenci podvodů je dobrá finanční gramotnost občanů České republiky, a právě o to se Česká národní banka a Finanční analytický úřad snaží.

8 Závěr

Bankovní sféra je rychle se měnícím prostředím a konkurenčním prostředím. Oblasti AML/CFT a platebních podvodů představují pro banku obrovská rizika. Cílem diplomové práce bylo seznámení se nejdříve s teoretickými východisky v oblasti AML/CFT, platebních podvodů a zabezpečení bankovních služeb v internetové síti. Díky teoretickým základům bylo poté možno charakterizovat prostřednictvím statistika a dat Komerční banky, a.s. aktuální pozici v oblasti boje prosti praní špinavých peněz a celkově podezřelým obchodům. Po analýze spojené s interními procesy v postupu proti boji s praním špinavých peněz bylo využití dat z Finančního analytického úřadu. Finanční analytický úřad hraje ve vyhodnocování podezřelých obchodů nejdůležitější roli, jelikož v případě shledání opravdu podezřelého obchodu je v jeho kompetenci uvalení sankcí nebo zmrazení finančních prostředků.

V dnešní době jsou platební podvody stále větším rizikem jak pro klienty bank, tak i pro kompletní bankovní systém. S nárůstem digitálních platebních metod a online transakcí se otevírá široké pole pro různé formy podvodů – phishing, krádeže identity a velice rozšířené kryptopodvody. Tyto podvody způsobují nejen finanční ztráty, ale také poškozují důvěru ve finanční systém. Klíčovými faktory ovlivňující aktuální stav platebních podvodů jsou rychlé technologické pokroky ve formě inovací a komplexních postupů. Nicméně na základě vyhodnocení dat se každoročně zvyšují počty podvodů, ale na druhé straně i počty zachráněných finančních prostředků klientů bank. Systémy jako jsou FDS jsou pro banky velice cenné a mohou být nejlepší prevencí proti platebním podvodům. Tyto technologie umožňují bankám lépe monitorovat a identifikovat podezřelé transakce v reálném čase, což zvyšuje účinnost detekce a prevence podvodů.

V závěru lze konstatovat, že platební podvody a obecně problematika AML/CFT představuje závažný problém pro společnost a pro finanční systém jako celek. Je nezbytné nejen sledovat aktuální trendy a inovace v problematických oblastech, ale také aktivně spolupracovat na vytváření a implementaci strategií pro ochranu celého finančního systému.

9 Seznam použitých zdrojů

1. BUCKLE, M.; BECCALLI, E. Principles of banking and finance. *Published by: University of London*, 2008.
2. CHAPMAN, Rose. *Anti-Money Laundering: A practical guide to reducing organizational risk*. Kogan Page Publishers, 2018.
3. DILL, Alexander. *Bank regulation, risk management, and compliance: theory, practice, and key problem areas*. informa law from Routledge, 2019.
4. DILL, Alexander. *Anti-money laundering regulation and compliance: Key Problems and Practice Areas*. Edward Elgar Publishing, 2021.
5. Electronic Banking: The Ultimate Guide to Business and Technology of Online Banking. Německo: Vieweg+Teubner Verlag, 2013.
6. EL Khoury, Chady. Countering the Financing of Terrorism: Good Practices to Enhance Effectiveness. (2023). Spojené státy americké: International Monetary Fund.
7. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561
8. MEJSTŘÍK, Michal; PEČENÁ, Magda a TEPLÝ, Petr. *Bankovnictví v teorii a praxi: Banking in theory and practice*. Praha: Karolinum, 2014. ISBN 978-80-246-2870-7.
9. JAMES, Lance. *Phishing exposed*. Elsevier, 2005. ISBN 978-1597490306
10. REVENDA, Zbyněk. *Centrální bankovnictví*. 3., aktualiz. vyd. Praha: Management Press, 2011. ISBN 978-80-7261-230-7.
11. REVENDA, Zbyněk. *Peněžní ekonomie a bankovnictví*. 4. vyd. Praha: Management Press, 2005. ISBN 978-80-7261-132-4.
12. SEDLÁČKOVÁ, Helena a BUCHTA, Karel. *Strategická analýza*. 2., přeprac. a dopl. vyd. C.H. Beck pro praxi. V Praze: C.H. Beck, 2006. ISBN 8071793671.

Seznam internetových zdrojů

1. CO JE EVIDENCE SKUTEČNÝCH MAJITELŮ. *Evidence skutečných majitelů* [online]. 2023 [cit. 2024-02-07]. Dostupné z: https://esm.justice.cz/ias/issm/napoveda#kdoJeSm
2. ČESKÁ NÁRODNÍ BANKA. *Státní banka československá* [online]. 2018 [cit. 2023-12-09]. Dostupné z: https://www.historie.cnb.cz/cs/dejiny_instituce/statni_banka_ceskoslovenska/index.html
3. CISCO. *What Is Phishing?* [online]. 2024 [cit. 2024-02-23]. Dostupné z: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html
4. ČESKÁ NÁRODNÍ BANKA. *Hlavní poslání centrální banky* [online]. 2018 [cit. 2023-12-09]. Dostupné z: https://www.cnb.cz/cs/menova-politika/vzdelavani/02-hlavni-poslani-centralni-banky/
5. ČESKÁ NÁRODNÍ BANKA. *O ČNB* [online]. 2024 [cit. 2023-12-09]. Dostupné z: https://www.cnb.cz/cs/o_cnb/
6. ČESKÁ NÁRODNÍ BANKA. Dohled nad finančním trhem [online].. 2024. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/. [cit. 2023-12-09].
7. ČESKÁ NÁRODNÍ BANKA. *Systémové riziko a kapitál českých bank* [online]. [cit. 2024-01-02]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Systemove-riziko-a-kapital-ceskych-bank/
8. ČESKÁ NÁRODNÍ BANKA. *Jaká je role ČNB v oblasti prevence praní špinavých peněz a financování terorismu?* [online]. 2024 [cit. 2024-01-02]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Jaka-je-role-CNB-v-oblasti-prevence-prani-spinavych-penez-a-financovani-terorismu/
9. ČESKÉ NOVINY. *První phishing v Česku, terčem byla CitiBank* [online]. [cit. 2024-02-20]. Dostupné z: https://www.ceskenoviny.cz/zpravy/178228
10. ENISA. *Phishing/Spear phishing* [online]. 2024 [cit. 2024-02-23]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing

11. EUROPEAN UNION, *The EU's work to tackle terrorism* [online]. 2024 [cit. 2024-02-06]. Dostupné z: https://www.consilium.europa.eu/en/eu-response-to-terrorism/
12. FATF. *What we do* [online]. 2024 [cit. 2024-01-05]. Dostupné z: https://www.fatf-gafi.org/en/the-fatf/what-we-do.html
13. FATF. *High-risk and other monitored jurisdictions* [online]. [cit. 2024-03-30]. Dostupné z: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html
14. FORBES. *What Is Smishing? Definition, Examples & Protection* [online]. [cit. 2024-02-21]. Dostupné z: https://www.forbes.com/advisor/business/what-is-smishing/
15. FINANČNÍ ANALYTICKÝ ÚŘAD. *Kdo jsme a co děláme?* [online]. 2022 [cit. 2024-01-05]. Dostupné z: https://fau.gov.cz/o-uradu#kdo-jsme-a-co-delame
16. FINANČNÍ ANALYTICKÝ ÚŘAD. *Úvod do problematiky* [online]. 2022 [cit. 2024-01-05]. Dostupné z: https://fau.gov.cz/legislativa-a-metodika-459
17. FINANČNÍ ANALYTICKÝ ÚŘAD. *FATF* [online]. 2022 [cit. 2024-01-06]. Dostupné z: https://fau.gov.cz/fatf
18. KOMERČNÍ BANKA, A.S. *Internetové bankovnictví MojeBanka* [online]. [cit. 2024-02-22]. Dostupné z: https://www.kb.cz/cs/nase-aplikace/mojebanka
19. KOMERČNÍ BANKA, A.S. *Bezpečnost* [online]. [cit. 2024-02-23]. Dostupné z: https://www.kb.cz/cs/podpora/bezpecnost
20. NOVINKY.CZ. *Podvodník s virtuální měnou donutil ženu k instalaci programu* [online]. [cit. 2024-02-21]. Dostupné z: https://www.novinky.cz/clanek/krimi-podvodnik-s-virtualni-menou-donutil-zenu-k-instalaci-programu-pak-ziskal-milion-40377548
21. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *NKÚIB* [online]. [cit. 2024-03-29]. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/
22. POLICIE ČR. *Ztráta identity* [online]. [cit. 2024-02-21]. Dostupné z: https://www.policie.cz/clanek/ztrata-identity.aspx
23. POLICIE ČR. *Vishing a spoofing* [online]. [cit. 2024-02-21]. Dostupné z: https://www.policie.cz/clanek/vishing-a-spoofing.aspx

24. PROOFPOINT. *What Is Vishing?* [online]. [cit. 2024-02-20]. Dostupné z: https://www.proofpoint.com/us/threat-reference/vishing
25. RAIFFEISEN BANK, A.S. *BEZPEČNÉ BANKOVNICTVÍ* [online]. 2024 [cit. 2024-02-22]. Dostupné z: https://www.rb.cz/bezpecne-bankovnictvi

Seznam legislativních zdrojů

1. Zákon č. 335/2002 Sb., o České národní bance.
2. Vyhláška č. 67/2018 Sb. o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu
3. Zákon č. 253/2008 Sb., zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
4. Zákon č. 37/2021 Sb., zákon o evidenci skutečných majitelů
5. Metodický pokyn č.7 FAÚ. Opatření vůči politicky exponovaným osobám

Seznam interních zdrojů

1. Vnitropodnikový manuál útvaru AML (Komerční banka, 2023)
2. Vnitropodnikový manuál útvaru AMLCOM (Komerční banka, 2023)
3. AML/CFT analysis (Komerční banka, 2023)
4. FCC dokument platebních podvodů (Komerční banka, 2023)

10 Seznam obrázků, tabulek, grafů a zkratek

10.1 Seznam obrázků

10.2 Seznam tabulek

10.3 Seznam grafů

10.4 Seznam použitých zkratek

AML – Anti-money laundering

AMLZ – Aml zákon

BaPo – Bankovní poradce

CFT – Combating the Financing of Terrorism

FATF – Financial Action Task Force

FDS – Fraud detecton systém

FO – Fyzická osoba

FSRB – Regionální uskupení FATF

IB – Internetové bankovnictví

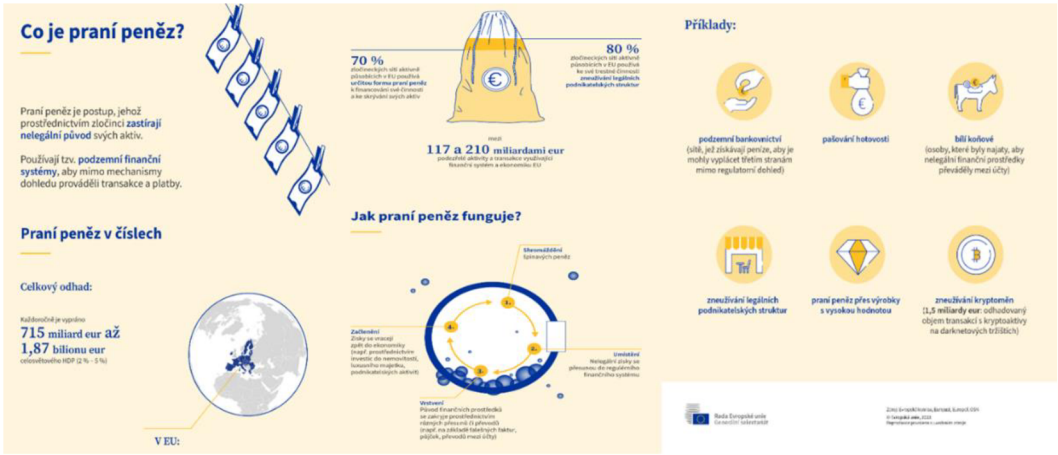
JPÚ – Jiná platební instituce

MONEYVAL – Výbor expertů pro hodnocení AML/CFT Rady Evropy

PO – Právnická osoba

11 Přílohy

Příloha č.1 – Infografika AML/CFT dle Evropské rady a Rady Evropské unie



Zdroj: Evropská unie,2023

Příloha č.2 – Vnitrostátní seznam funkcí PEP:

Prezident republiky + vedoucí Kanceláře prezidenta republiky
Předseda vlády
Vedoucí ústředního orgánu státní správy a jeho zástupce (náměstek, státní tajemník):
- ministerstvo – ministr, náměstek ministra, státní tajemník,
- Český statistický úřad – předseda, místopředsedové,
- Český úřad zeměměřický a katastrální – předseda, místopředseda,
- Český báňský úřad – předseda, zástupce předsedy – ředitel sekce báňské správy,
- Úřad průmyslového vlastnictví – předseda, zástupce,
- Úřad pro ochranu hospodářské soutěže – předseda, místopředsedové,
- Správa státních hmotných rezerv – předseda, zástupce,
- Státní úřad pro jadernou bezpečnost – předsedkyně, ředitelé sekcí,
- Národní bezpečnostní úřad – ředitel, náměstci ředitele,
- Energetický regulační úřad – předseda Rady ERÚ, členové Rady ERÚ,
- Úřad vlády České republiky – vedoucí Úřadu vlády, náměstek pro řízení sekce, státní tajemník,
- Český telekomunikační úřad – předsedkyně Rady ČTÚ, členové Rady ČTÚ,
- Úřad pro ochranu osobních údajů – předsedkyně, místopředseda,
- Úřad pro dohled nad hospodařením politických stran a politických hnutí – předseda, členové Úřadu,
- Národní úřad pro kybernetickou a informační bezpečnost – ředitel, náměstci,

Člen Parlamentu České republiky
- poslanec, senátor, vedoucí Kanceláře Poslanecké sněmovny, vedoucí Kanceláře Senátu,

Člen řídícího orgánu politické strany a politického hnutí – předseda, místopředsedové,
Vedoucí představitel územní samosprávy
- primátor, náměstek primátora, tajemník magistrátu, ředitel Magistrátu hlavního města Prahy, hejtman, náměstek hejtmana, ředitel krajského úřadu, starosta obce s rozšířenou působností, starosta městské části hlavního města Prahy uvedené v § 4 odst. 1 obecně závazné vyhlášky č. 55/2000 Sb. hl. m. Prahy, kterou se vydává Statut hlavního města Prahy,

Soudce nejvyššího soudu, ústavního soudu nebo jiného nejvyššího justičního orgánu, proti jehož rozhodnutí obecně až na výjimky nelze použít opravné prostředky
-soudce Ústavního soudu, soudce Nejvyššího správního soudu, soudce Nejvyššího soudu, nejvyšší státní zástupce,

Člen bankovní rady centrální banky
- guvernér, viceguvernér, člen bankovní rady České národní banky,

Vysoký důstojník ozbrojených sil nebo sboru
- Policie České republiky – policejní prezident, ředitelé krajských ředitelství Policie České republiky, Generální inspekce bezpečnostních sborů – ředitel, Bezpečnostní informační služba – ředitel, Vojenské zpravodajství – ředitel, Úřad pro zahraniční styky a informace – ředitel, Armáda České republiky – náčelník Generálního štábu Armády České republiky, ředitelé krajských vojenských velitelství, Hradní stráž – velitel, Vojenská kancelář prezidenta republika – náčelník,

Člen nebo zástupce člena, je-li jím právnická osoba, statutárního orgánu obchodní korporace ovládané státem
- člen představenstva, stejně jako každý další člen správního, řídícího nebo kontrolního orgánu obchodní korporace ve vlastnictví státu (obchodní korporace, v níž Česká republika přímo nebo nepřímo vlastní více jak 50% podíl),

Ředitel a zástupce ředitele státního podniku, členové dozorčí rady státního podniku
Ředitel a zástupce ředitele Všeobecné zdravotní pojišťovny České republiky, členové správní rady a členové dozorčí rady VZP ČR

Zdroj: metodický pokyn č.7 FAÚ,2020

Příloha č.3 – MED-HIGH/HIGH rizikové země

COUNTRY NAME	Financial Crime RATING*	COUNTRY NAME	Financial Crime RATING*	COUNTRY NAME	Financial Crime RATING*	COUNTRY NAME	Financial Crime RATING*
AFGHANISTAN	HIGH	KYRGYZSTAN	HIGH	EQUATORIAL GUINEA	HIGH	SAMOA	HIGH
ALBANIA	HIGH	LAOS	HIGH	ERITREA	HIGH	SAO TOME AND PRINCIPE	HIGH
ALGERIA	HIGH	LEBANON	HIGH	ETHIOPIA	HIGH	SAUDI ARABIA	MEDHIGH
AMERICAN SAMOA	HIGH	LESOTHO	HIGH	FAROE ISLANDS	MEDHIGH	SENEGAL	HIGH
ANGOLA	HIGH	LIBERIA	HIGH	FIJI	HIGH	SERBIA	HIGH
ANGUILLA	HIGH	LIBYA	HIGH	GABON	HIGH	SEYCHELLES	HIGH
ANTIGUA AND BARBUDA	MEDHIGH	LIECHTENSTEIN	MEDHIGH	GAMBIA	HIGH	SIERRA LEONE	HIGH
ARGENTINA	MEDHIGH	MACAO	MEDHIGH	GEORGIA	MEDHIGH	SOLOMON ISLANDS	HIGH
ARMENIA	HIGH	MADAGASCAR	HIGH	GHANA	HIGH	SOMALIA	HIGH
ARUBA	MEDHIGH	MALAWI	HIGH	GIBRALTAR	MEDHIGH	SOUTH AFRICA	MEDHIGH
AZERBAIJAN	HIGH	MALAYSIA	MEDHIGH	GREENLAND	MEDHIGH	SOUTH SUDAN	HIGH
BAHAMAS	HIGH	MALDIVES	HIGH	GRENADA	MEDHIGH	SRI LANKA	HIGH
BAHRAIN	MEDHIGH	MALI	HIGH	GUAM	HIGH	ST HELENA	HIGH
BANGLADESH	HIGH	MALTA	HIGH	GUATEMALA	HIGH	ST KITTS AND NEVIS	MEDHIGH
BARBADOS	HIGH	MARSHALL ISLANDS	MEDHIGH	GUERNSEY	MEDHIGH	ST LUCIA	MEDHIGH
BELARUS	HIGH	MAURITANIA	HIGH	GUINEA	HIGH	ST MAARTEN	HIGH
BELIZE	HIGH	MAURITIUS	HIGH	GUINEA-BISSAU	HIGH	ST VINCENT AND THE GRENADINES	MEDHIGH
BENIN	HIGH	MEXICO	HIGH	GUYANA	HIGH	SUDAN	HIGH
BERMUDA	MEDHIGH	MICRONESIA (FEDERATED STATES OF)	HIGH	HAITI	HIGH	SURINAME	HIGH
BHUTAN	MEDHIGH	MOLDOVA (REPUBLIC OF)	HIGH	HONDURAS	HIGH	SWAZILAND (ESWATINI)	HIGH
BOLIVIA	HIGH	MONACO	MEDHIGH	HUNGARY	MEDHIGH	SYRIA	HIGH
BOSNIA AND HERZEGOVINA	HIGH	MONGOLIA	HIGH	INDIA	MEDHIGH	TAIWAN	MEDHIGH
BOTSWANA	HIGH	MONTENEGRO	MEDHIGH	INDONESIA	MEDHIGH	TAJIKISTAN	HIGH
BRAZIL	MEDHIGH	MONTSERRAT	MEDHIGH	IRAN	HIGH	TANZANIA	HIGH
BRUNEI DARUSSALAM	MEDHIGH	MOROCCO	HIGH	IRAQ	HIGH	THAILAND	HIGH
BURKINA FASO	HIGH	MOZAMBIQUE	HIGH	ISLE OF MAN	MEDHIGH	TIMOR-LESTE	HIGH
BURUNDI	HIGH	MYANMAR	HIGH	IVORY COAST	HIGH	TOGO	HIGH
CAMBODIA	HIGH	NAMIBIA	HIGH	JAMAICA	HIGH	TONGA	HIGH
CAMEROON	HIGH	NAURU	MEDHIGH	JERSEY	MEDHIGH	TRINIDAD AND TOBAGO	HIGH
CAPE VERDE	MEDHIGH	NEPAL	HIGH	JORDAN	HIGH	TUNISIA	HIGH
CAYMAN ISLANDS	HIGH	NICARAGUA	HIGH	KAZAKHSTAN	HIGH	TURKEY	HIGH
CENTRAL AFRICAN REPUBLIC	HIGH	NIGER	HIGH	KENYA	HIGH	TURKMENISTAN	HIGH
CHAD	HIGH	NIGERIA	HIGH	KIRIBATI	HIGH	TURKS AND CAICOS ISLANDS	MEDHIGH
CHINA	MEDHIGH	NIUE	MEDHIGH	KOREA (DEM PEOPLE'S REPUBLIC OF)	HIGH	TUVALU	HIGH
COLOMBIA	HIGH	NORTHERN MACEDONIA	MEDHIGH	KOSOVO	HIGH	UGANDA	HIGH
COMOROS	HIGH	NORTHERN MARIANA ISLANDS	HIGH	KUWAIT	HIGH	UKRAINE	HIGH

CONGO	HIGH	OMAN	HIGH	VIETNAM	HIGH	UNITED ARAB EMIRATES	HIGH
CONGO (DEMOCRATIC REPUBLIC OF THE)	HIGH	PAKISTAN	HIGH	VIRGIN ISLANDS, BRITISH	MEDHIGH	UZBEKISTAN	HIGH
COSTA RICA	MEDHIGH	PALAU	HIGH	VIRGIN ISLANDS, U.S.	HIGH	VANUATU	HIGH
CROATIA	MEDHIGH	PALESTINE AUTHORITY	HIGH	YEMEN	HIGH	VENEZUELA	HIGH
CUBA	HIGH	PANAMA	HIGH	ZAMBIA	HIGH	ZIMBABWE	HIGH
CURACAO	MEDHIGH	PAPUA NEW GUINEA	HIGH	JAMAICA	HIGH	TONGA	HIGH
CYPRUS	MEDHIGH	PARAGUAY	HIGH	JERSEY	MEDHIGH	TRINIDAD AND TOBAGO	HIGH
DJIBOUTI	HIGH	PERU	MEDHIGH	JORDAN	HIGH	TUNISIA	HIGH
DOMINICA	HIGH	PHILIPPINES	HIGH	KAZAKHSTAN	HIGH	TURKEY	HIGH
DOMINICAN REPUBLIC	MEDHIGH	QATAR	MEDHIGH	KENYA	HIGH	TURKMENISTAN	HIGH
ECUADOR	HIGH	ROMANIA	MEDHIGH	KIRIBATI	HIGH	TURKS AND CAICOS ISLANDS	MEDHIGH
EGYPT	HIGH	RUSSIAN FEDERATION	HIGH	KOREA (DEM PEOPLE'S REPUBLIC OF)	HIGH	TUVALU	HIGH
EL SALVADOR	HIGH	RWANDA	HIGH	KOSOVO	HIGH	UGANDA	HIGH
EQUATORIAL GUINEA	HIGH	SAMOA	HIGH	KUWAIT	HIGH	UKRAINE	HIGH
ERITREA	HIGH	SAO TOME AND PRINCIPE	HIGH	VIETNAM	HIGH	UNITED ARAB EMIRATES	HIGH
ETHIOPIA	HIGH	SAUDI ARABIA	MEDHIGH	VIRGIN ISLANDS, BRITISH	MEDHIGH	UZBEKISTAN	HIGH
FAROE ISLANDS	MEDHIGH	SENEGAL	HIGH	VIRGIN ISLANDS, U.S.	HIGH	VANUATU	HIGH
FIJI	HIGH	SERBIA	HIGH	YEMEN	HIGH	VENEZUELA	HIGH
GABON	HIGH	SEYCHELLES	HIGH	ZAMBIA	HIGH	ZIMBABWE	HIGH
GAMBIA	HIGH	SIERRA LEONE	HIGH	INDONESIA	MEDHIGH	TAJIKISTAN	HIGH
GEORGIA	MEDHIGH	SOLOMON ISLANDS	HIGH	IRAN	HIGH	TANZANIA	HIGH
GHANA	HIGH	SOMALIA	HIGH	IRAQ	HIGH	THAILAND	HIGH
GIBRALTAR	MEDHIGH	SOUTH AFRICA	MEDHIGH	ISLE OF MAN	MEDHIGH	TIMOR-LESTE	HIGH
GREENLAND	MEDHIGH	SOUTH SUDAN	HIGH	IVORY COAST	HIGH	TOGO	HIGH
GRENADA	MEDHIGH	SRI LANKA	HIGH	JAMAICA	HIGH	TONGA	HIGH
GUAM	HIGH	ST HELENA	HIGH	JERSEY	MEDHIGH	TRINIDAD AND TOBAGO	HIGH
GUATEMALA	HIGH	ST KITTS AND NEVIS	MEDHIGH	JORDAN	HIGH	TUNISIA	HIGH
GUERNSEY	MEDHIGH	ST LUCIA	MEDHIGH	KAZAKHSTAN	HIGH	TURKEY	HIGH
GUINEA	HIGH	ST MAARTEN	HIGH	KENYA	HIGH	TURKMENISTAN	HIGH
GUINEA-BISSAU	HIGH	ST VINCENT AND THE GRENADINES	MEDHIGH	KIRIBATI	HIGH	TURKS AND CAICOS ISLANDS	MEDHIGH
GUYANA	HIGH	SUDAN	HIGH	KOREA (DEM PEOPLE'S REPUBLIC OF)	HIGH	TUVALU	HIGH
HAITI	HIGH	SURINAME	HIGH	KOSOVO	HIGH	UGANDA	HIGH
HONDURAS	HIGH	SWAZILAND (ESWATINI)	HIGH	KUWAIT	HIGH	UKRAINE	HIGH
HUNGARY	MEDHIGH	SYRIA	HIGH	VIETNAM	HIGH	UNITED ARAB EMIRATES	HIGH
INDIA	MEDHIGH	TAIWAN	MEDHIGH	VIRGIN ISLANDS, BRITISH	MEDHIGH	UZBEKISTAN	HIGH
ZAMBIA	HIGH	ZIMBABWE	HIGH	VIRGIN ISLANDS, U.S.	HIGH	VANUATU	HIGH
				YEMEN	HIGH	VENEZUELA	HIGH

Zdroj: FATF,2023