



Adastra Fraud Management System

Adastra Fraud Management System (AFMS) je aplikace vyvinutá firmou Adastra jako podpůrný nástroj pro odhalování podvodů. Uplatnění nalézá zejména v pojišťovnictví, bankovníctví a telekomunikacích, ale díky obecnosti řešení a nastavitelnosti ji lze nasadit i v jiných oblastech.

Value Proposition		Business přínosy řešení
<p>■ Pojišťovny Pojistné podvody způsobují pojišťovnám velké finanční ztráty a jejich četnost narůstá. Podle České asociace pojišťoven vzrostl v letech 2000 – 2004 počet nahlášených případů pojistného podvodu ze 408 na 1015 (ročně). Podle odhadů odborníků je zhruba každá desátá nahlášená pojistná událost pokusem o podvod a jejich objem se pohybuje ve stovkách milionů korun. Problematika pojistného podvodu byla proto zařazena mezi hlavní úkoly České asociace pojišťoven pro rok 2005. U veřejnosti převládá představa o malé riskantnosti pojistného podvodu a stále jej považuje za nepříliš vážný trestný čin. Z pohledu pojišťoven se zase může zdát, že je levnější některé případy proplatit, než vést nákladné vyšetřování a soudní proces. AFMS se uplatní při pravidelném vyhodnocování nestandardních pojistných událostí a smluv na základě analýz klientů, předmětu pojištění, ziskatelů i likvidátorů. Tím dochází k vyšší kontrole, omezení rizik a zvýšení efektivity činnosti vyšetřování.</p> <p>■ Banky Mezi nejčastější podvody v bankovním sektoru patří zneužití platebních karet a legalizace výnosů z trestné činnosti. Podle statistiky Finančního analytického útvaru Ministerstva financí České republiky byla v rámci boje proti praní peněz v roce 2002 podána trestní oznámení na celkovou částku téměř 1,5 mld. Kč.</p>	<p>Opatření k problematice boje proti praní peněz jsou zakotvena v zákonu číslo 61/1996 Sb. a konkretizována v požadavcích na vnitřní řídicí a kontrolní systém banky Opatřením České národní banky č. 1 ze dne 8. září 2003, 2. Opatřením ČNB č. 2 ze dne 3. února 2004 a 16. Úředním sdělením ČNB ze dne 8. června 2004. AFMS je nasazeno se speciálními úpravami již v několika bankách v ČR jako nástroj boje proti praní špinavých peněz.</p> <p>■ Telekomunikace Mezi nejčastější podvody v telekomunikacích patří získání a používání služeb bez úmyslu zaplatit (včetně podvodů v rámci roamingu), nebo zneužívání dotovaných a jiných marketingových akcí. Dalším problémem jsou podvody prováděné zaměstnanci a nespolehlivými obchodními partnery, který provází stejně tak i bankovní sektor a pojišťovny. AFMS poskytuje účinnou pomoc při pravidelném vyhodnocování nestandardních událostí, odhalování podezřelých případů a nabízí i cestu k předcházení podvodů a ztrát z nich. Nasazení AFMS v telekomunikacích typicky zahrnuje near online agregace CDRs stejně jako dlouhodobé vyhodnocování chování zákazníka a vyhodnocování jeho aktuálního chování v tomto kontextu (často volaná čísla, směry volání, místa volání...).</p>	<p>■ Úspory – snížením objemu podvodů a prevencí jejich vzniku.</p> <p>■ Konkurenční výhoda na trhu – systém pro podporu odhalování podvodů může být rozhodujícím faktorem pro získání výhody nad konkurencí.</p> <p>■ Snížení zátěže IT – potřebné reporty si v AFMS vytváří uživatelé samostatně. Reporty mohou být generovány automaticky v nastavených intervalech i near online. Odpadají tak náročné a opakované úlohy, které dříve zpracovávalo IT oddělení.</p> <p>■ Důvěryhodnost – na podvodníky doplácí poctivá část klientů pojišťoven. Boj proti podvodům tak neznamená pro pojišťovnu pouze ušetřené peníze, ale zároveň i zlepšení obchodního jména a spokojenost klientů.</p> <p>■ Podpora plnění podmínek ČNB – implementace AFMS směřuje ke splnění požadavků ČNB na vnitřní řídicí a kontrolní systém banky.</p> <p>■ Zvýšení revenue – včasná identifikace podvodu a zabránění zneužívání služeb sníží náklady a tím zvýší zisk telekomunikačních firem.</p> <p>■ Cenově efektivní řešení – díky modulárnímu uspořádání řešení, které může realizovat část řešení na již existující technologické infrastruktuře datového skladu, je dosaženo optimálního využití předchozích investic a z toho plynoucích cenových úspor.</p>

Popis řešení		Vlastnosti řešení
<p>AFMS</p> <ul style="list-style-type: none"> AFMS je uživatelská aplikace navržená pro podporu odhalování podvodů a postavená na přípravě dat v datovém skladu či ODS (Operational Data Store). Nachází uplatnění zejména v pojišťovnách, bankách a telekomunikačních firmách. <p>Indikátory, skóre, váhy</p> <ul style="list-style-type: none"> Podvod je ve většině případů charakterizován určitým typickým chováním subjektů. Pro rozpoznání nebezpečí rizika podvodu je třeba vystavět soubor pravidel, který povede k rozpoznání takové události. Roli pravidel v aplikaci AFMS zastávají tzv. indikátory. U každého indikátoru lze nastavit intervaly hodnot s bodovým ohodnocením jejich rizikovosti. Význam indikátoru může být upraven přiřazením váhy. Významnou funkcionalitou AFMS je možnost použít již vytvořené indikátory při tvorbě nových a vystavět tak jednoduše komplexní hodnotící schéma. <p>Filtry</p> <ul style="list-style-type: none"> Pomocí filtrů se hodnotí entity, u nichž hrozí nebezpečí podvodu. Základním stavebním prvkem filtrů jsou indikátory. Součtem bodových ohodnocení indikátorů zařazených do filtru se identifikují podezřelé případy, které jsou následně vygenerovány do reportu pro další posouzení. 	<ul style="list-style-type: none"> Změny nastavení filtru se provádí vytvořením nové verze filtru, díky čemuž jsou kdykoli dostupné původní verze. Jednotlivé verze filtrů se mohou nacházet v různých stavech (pracovní, testovací, produkční aktuální a produkční neaktuální) a podle toho je omezena množina operací, které s nimi lze provádět. <p>Reporty</p> <ul style="list-style-type: none"> Report obsahuje podezřelé případy vyhodnocené na základě použité verze filtru k určitému časovému rozmezí. K dispozici je zobrazení detailu každého případu se seznamem bodových ohodnocení použitých indikátorů. K reportu lze vždy dohledat nastavení verze filtru s příslušnými indikátory, datum vytvoření a jeho autora. <p>Workflow</p> <ul style="list-style-type: none"> Každý uživatel aplikace AFMS se musí autorizovat přístupovým jménem a heslem. Poté mu aplikace přiřadí uživatelská práva podle skupiny, do které je zařazen. S dostatečnými právy může uživatel k identifikovaným případům zadávat úkoly jiným uživatelům, nebo jejich skupinám, a sledovat odpovědi od pověřených zaměstnanců. Celý proces workflow aplikace dokumentuje. 	<ul style="list-style-type: none"> Použití metadat – AFMS staví na metadatech, která zahrnují definici proměnných, indikátorů, jejich hodnoty, bodové ohodnocení, nastavení filtrů apod. Flexibilita a modifikovatelnost – uživatelé mohou přefigurovat nastavení metadat a přizpůsobit tak aplikaci svým potřebám. Bezpečnost – vzhledem k citlivosti problematiky podvodů je bezpečnost řešena hned ve dvou úrovních: <ul style="list-style-type: none"> Databázová přístupová práva chrání metadata, což zaručuje bezpečnost všech provedených nastavení a konfigurací indikátorů a filtrů. Přístupová práva osob oprávněných pro práci v aplikaci AFMS a jejich zařazení do uživatelských skupin zaručuje přístup pouze k potřebné funkcionalitě pro daného pracovníka. Audit všech důležitých operací poskytuje záznam o práci každého uživatele. Díky tomuto monitoringu jsou vždy dostupné podklady pro případnou kontrolu. Podpora efektivní práce pomocí workflow – po identifikaci podezřelého případu začíná jeho prošetřování. Díky integrovanému workflow je jednoduché delegovat případy k řešení dalším zaměstnancům a sledovat informace podávané o průběhu jejich práce.

Základní architektura nasazení systému AFMS v pojišťovně



ADAstra, s.r.o.
Nile House
Karolinská 654/2
186 00 Praha 8 – Karlín
Tel.: +420 271 733 303
sales@adastra.cz www.adastra.cz