KPMG

KOCKÁZATKEZELÉS

Gyanús tranzakciók nyomában

Számítógépes csalásfelderítés

Gaidosch Tamás

2010. február 23.

AUDIT ▪ TAX ▪ ADVISORY

Tartalom

- Miért nehéz az auditoroknak észrevenni a csalást?
- Az IT rendszerek szerepe
- Példák

Okok


Álcázás és megtévesztés
Az elkövetők kontrollkörnyezeti ismeretei
Túl kicsi mintaméret
Miért nehéz az auditoroknak észrevenni a csalást?
Ráhangolódás hiánya (a csalás természetrajzának hiányos ismerete)
Nem elég erős szkepticizmus
Az átfogó kép hiánya
Hatékony ERM integráció hiánya
Hatékony felderítési eszköztár hiánya
Emocionális reakció a menedzsment részéről
Túlzott veszteségekben elrejetett esetek

A csalás természetrajza

Miért nehéz az auditoroknak észrevenni a csalást?

Álcázás és megtévesztés

Az elkövetők szándékosan félrevezető magatartása

Összevetve a hibázással: a nyomok megtervezett eltüntetése

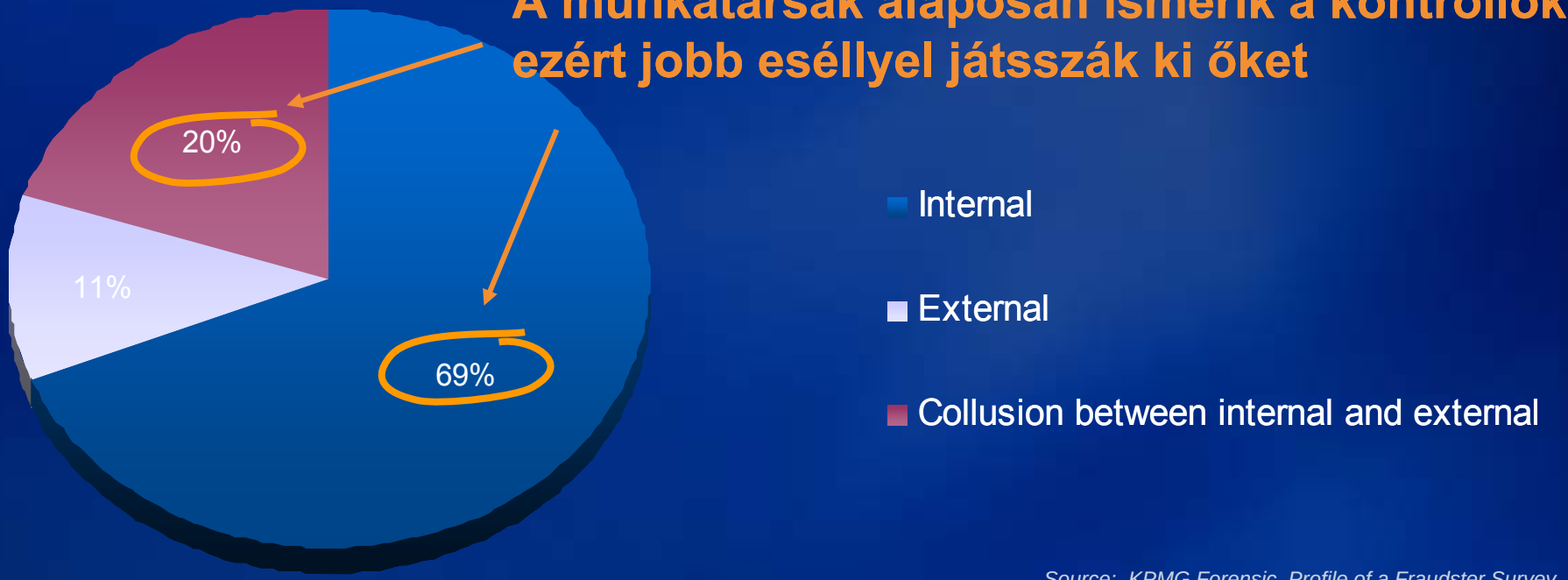
Hamis adatszolgáltatás: például nem elég gondos riport lekérések esetén

Az elkövetők kontrollkörnyezeti ismeretei

Az elkövetők viszonya a megkárosított intézménnyel:

Az esetek 89%-ában van belső résztvevő!

A munkatársak alaposan ismerik a kontrollokat, ezért jobb eséllyel játsszák ki őket



Source: KPMG Forensic, Profile of a Fraudster Survey

Emocionális reakció a menedzsment részéről

A csalás inherensen erős érzelmeket kiváltó téma – a menedzsment nem szereti, ha ez felmerül / felvetődik a saját területükön.

Milyen hatása van ennek?

- **A menedzsment gyakran működési veszteségekben „keni el” a csalás által okozott kárt**
- **Ezért az auditra való felkészülés során az auditorok tévesen ítélik meg a kockázatot**
- **Emiatt csökken a szkepticizmus, ami a csalási esetek kiszűrésére tervezett eljárások hatókörének és hatásosságának csökkenésében nyilvánul meg**
- **A felső vezetés nem figyel fel a csalás okozta károkra, ezért nem látnak okot a felderítésre / megelőzésre szánt erőforrások növelésére**

Példa: olajipar

Könyvelés	Menedzsment kifogás	Valódi ok
Üzemi veszteségek	Párolgás a tárolókból	Lopás a tárolókból (megfelelő szigetelés csökkenti a párolgást)
Rebranding	A csővezeték által okozott veszteség	Lopás a tárolókból és szállítás közben (rebranding eleve alacsony %)
Nem allokált veszteség	Karbantartás miatti veszteségek a kutaknál	Lopás a kutaknál (az ilyen veszteség minimális)
Kontrakció	Hőmérséklet-különbségek miatti térfogatcsökkenés	Lopás a tárolókból és szállítás közben (kompenzáció és térfogatnövekedés is van)

…tapasztalat nélkül nehéz eldönteni, hogy a veszteség reális-e, vagy túlzott

Az auditor természetrajza és tapasztalata

Miért nehéz az auditoroknak észrevenni a csalást?

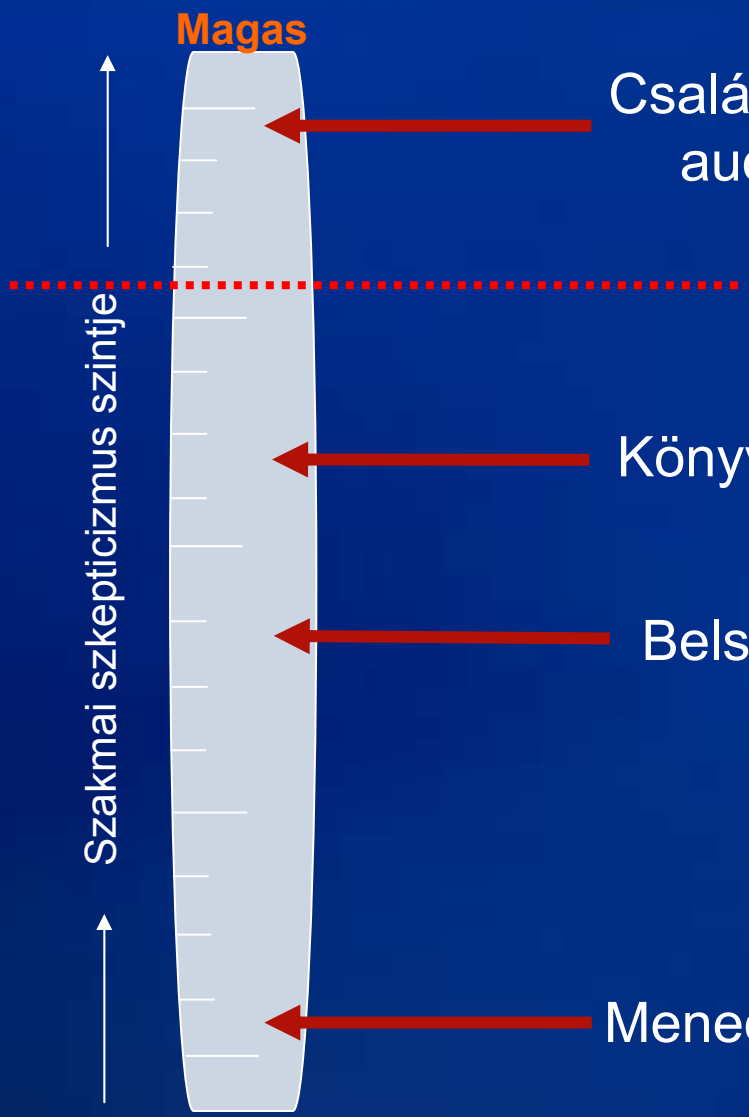
Előzetes ismeretek és kitettség

Egyszerű példa:
Várandós feleségemmel vásárolva egy idő után feltűnt, hogy több várandós nő van a bevásárlóközpontban.

Gondolatmenet:
Vajon ezek a nők nem léteztek eddig, vagy inkább arról van szó, hogy a jelenlegi személyes tapasztalatom fogékonnyá tett, és ezért jobban észreveszem őket?

…Ha az audit csapatunk nem megfelelően tapasztalt csalási esetek vizsgálatában, várható-e, hogy munkájuk során elég érzékenyek lesznek az árulkodó jelekre?

Nem elég erős szkepticizmus



Csalásfelderítő auditorok

- nem bánják, ha gyűlölik őket
- nincs előzetes kapcsolat

Könyvvizsgálók

- jól bírják a népszerűtlenséget
- általában van előzetes kapcsolat

Belső ellenőrök

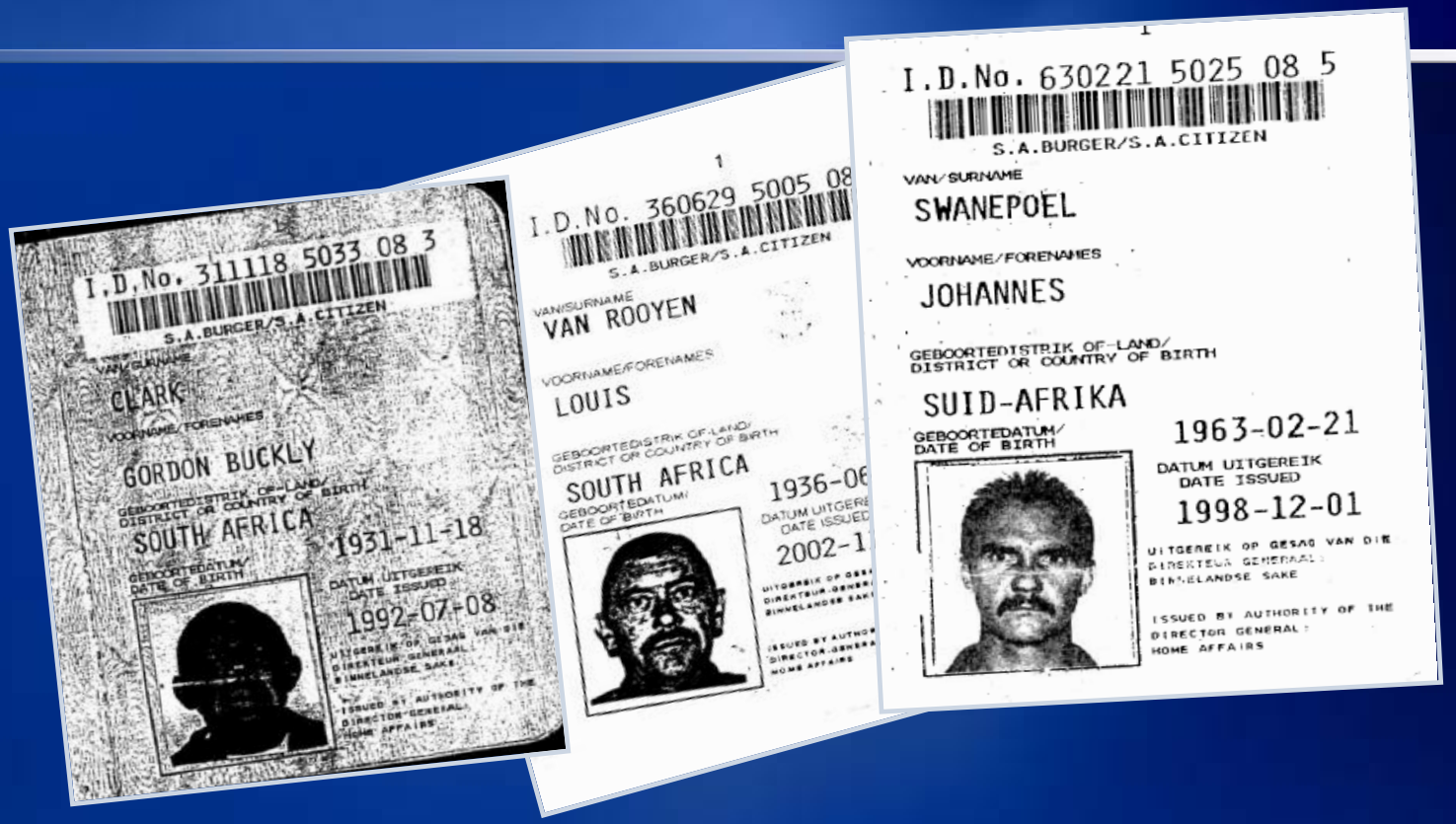
- elviselik a népszerűtlenséget
- kapcsolati háló

Menedzsment

- nehezen viselik a népszerűtlenséget
- erős kapcsolati háló

Hatékony felderítési eszköztár hiánya

Melyik hamis?



Van-e megfelelő szakismeret az audit csapatban, hogy hatásos csalásfelderítő audit teszteket tervezzenek meg?

Túl kicsi mintaméret

A hibák gyakoribbak a csalásoknál (általában)

A csalásokat gyakran nehezebb felderíteni a hibáknál

Tehát a gyanús tranzakciók hatásos felderítéséhez a szokványosnál lényegesen nagyobb mintaméret szükséges.

Két jónak tartott módszer:

- **Folyamatos audit monitoring**
- **Proaktív csalásfelderítő adatelemzés**

KPMG

Az átfogó kép hiánya

Példa – pénzügyi osztály audit

Főkönyv, számlák és megrendelések rekonsziliációja mintavétel alapján.

Tény: Két esetben nincs megrendelő a számlák mögött, bevétel könyvelve.

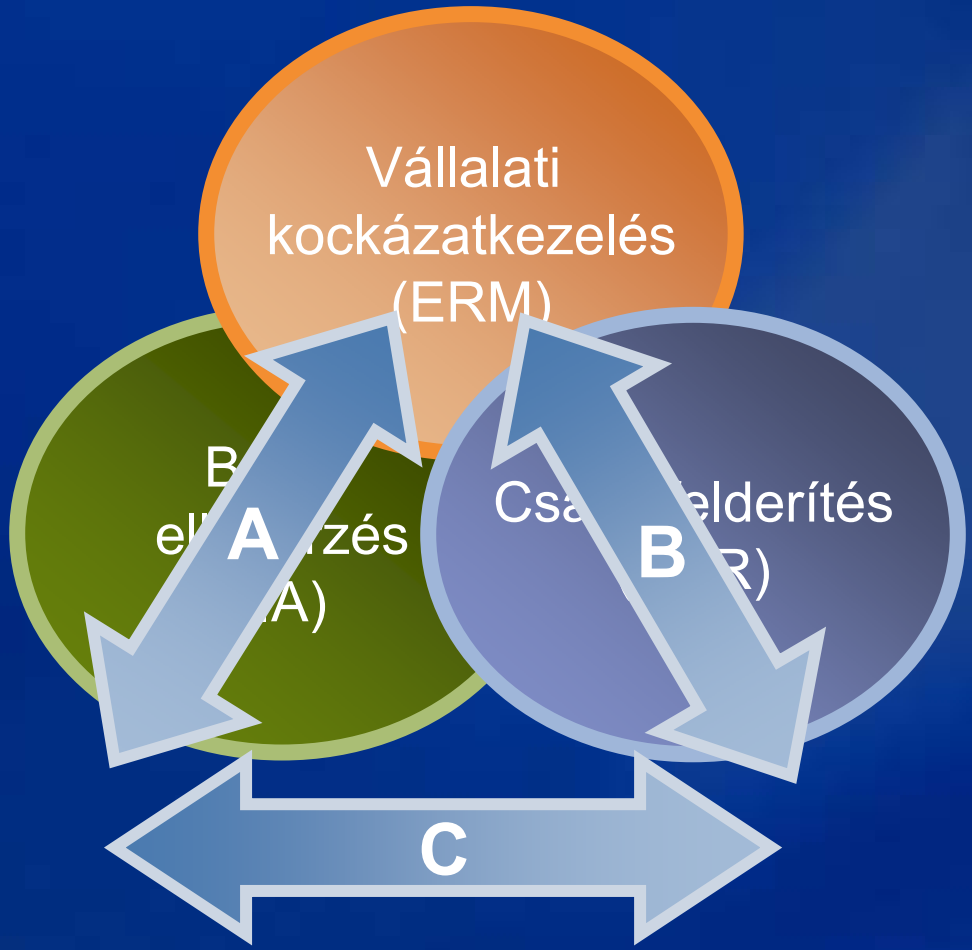
Rutin ellenőrzés: Újra elvesztették a dokumentációt! Adminisztratív hiba. Tipikus megállapítás: “25-ből 2 megrendelés dokumentációja nem található meg”.

Csalásfelderítés: Számla validálás és bank rekonsziliáció szükséges! (Hamis számlázás, számviteli csalás gyanúja.)

A folyamatok és struktúrák természetrajza

Miért nehéz az auditoroknak észrevenni a csalást?

Mennyire integrált a vállalatirányítás (governance)?



Hatékony ERM integráció hiánya

A & B
Vállalati kockázat-kezelés (ERM)

A csalás kockázatának stratégiai szinten, részletezettség nélkül való kezelése

- Az ERM-en nincs fraud tapasztalat
- Forensic / Fraud management nem vesz részt a kockázatelemzésben
- A folyamat szintű csalási kockázatok értékelésének hiánya
- Nem definiált csalási kockázati mutatók

Enterprise Risk Management – Risk Register

No.	Risk Description	Likelihood	Impact	Inherent Risk	Mitigating Controls	Control Effectiveness	Residual Risk	Priority	Management comments/proposed action plan
1	Risk of fraud	Likely	Serious	33	o Whistleblowing line o Fraud policy o Tone from the top	Good	6.5	Priority 5	Not applicable - within acceptable risk appetite

Irányítás integráció: példa a problémára

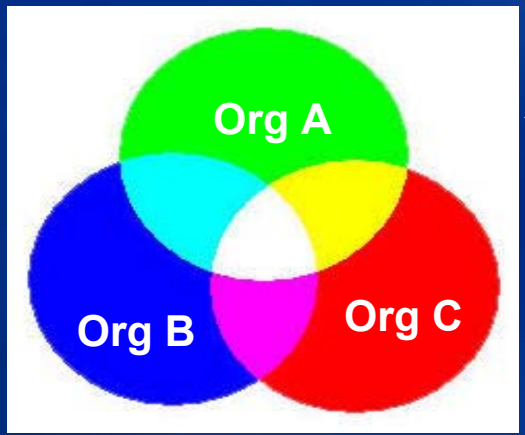
Alapfok:

- Biztonsági szervezet
- Fraud management
- Kockázatkezelés
- Belső ellenőrzés

Ki miért felel?

Nehezítés középfokon: nemzetközi mátrix-szervezet

Nehezítés felsőfokon: outsourcing-al kombinálva



Teljes felelősség

IT rendszerek szerepe

IT rendszerekkel elkövetett csalások

Számítógépes csalásfelderítés

Mintavétel vagy teljeskörű ellenőrzés?

Mintavételezés	Teljeskörű ellenőrzés
Előzetes kockázati becslés szükséges	Előzetes kockázati becslés nem szükséges
Elvárt konfidencia szintből levezetett mintaméret (többé-kevésbé tudományos)	Maximális konfidencia
Valódi véletlenszerű mintavétel ritka a gyakorlatban	N/A
Nem egyértelmű tennivalók gyanús találatok esetén	Egyértelmű tennivalók gyanús találatok esetén
Könnyebb kivitelezni	Nehezebb kivitelezni
Kézi módszerek lehetségesek	Kézi módszerek ritkán használhatók

Eszközök

CAAT: Computer Assisted Audit Tool

- Hatalmas adatmennyiségek kezelése
- Széles interfészelési (adatbeolvasási) lehetőségek
  - minden elterjedt platformhoz csatlakozhat
- Saját programnyelv
- Számos speciális funkció (például trendelemzéshez, korosításhoz)
- Detektív kontroll!

Példák: ACL, IDEA

CAAT példa: főkönyvi feladások vizsgálata

Jellemzően több százezer / millió rekord

Viszonylag egyszerű leválogatások

Eredmény: néhány száz / ezer további vizsgálatra érdemes feladás

Előnyök:

- teljes konfidencia (a definiált tesztekre értve)
- automatizált

Hátrányok:

- Adatok beszerzése, kezelése, konverziója nehézkes, időigényes
- Teljes körűség nem mindig garantált
- Hibák előfordulhatnak (de jellemzően könnyen észrevehetők)

CAAT példa: főkönyvi feladások vizsgálata

[vizsgálatok eredményeinek bemutatása –

három eset a KPMG gyakorlatából]

Családelemzés szoftveres támogatással

Strukturált és strukturálatlan információk összegyűjtése

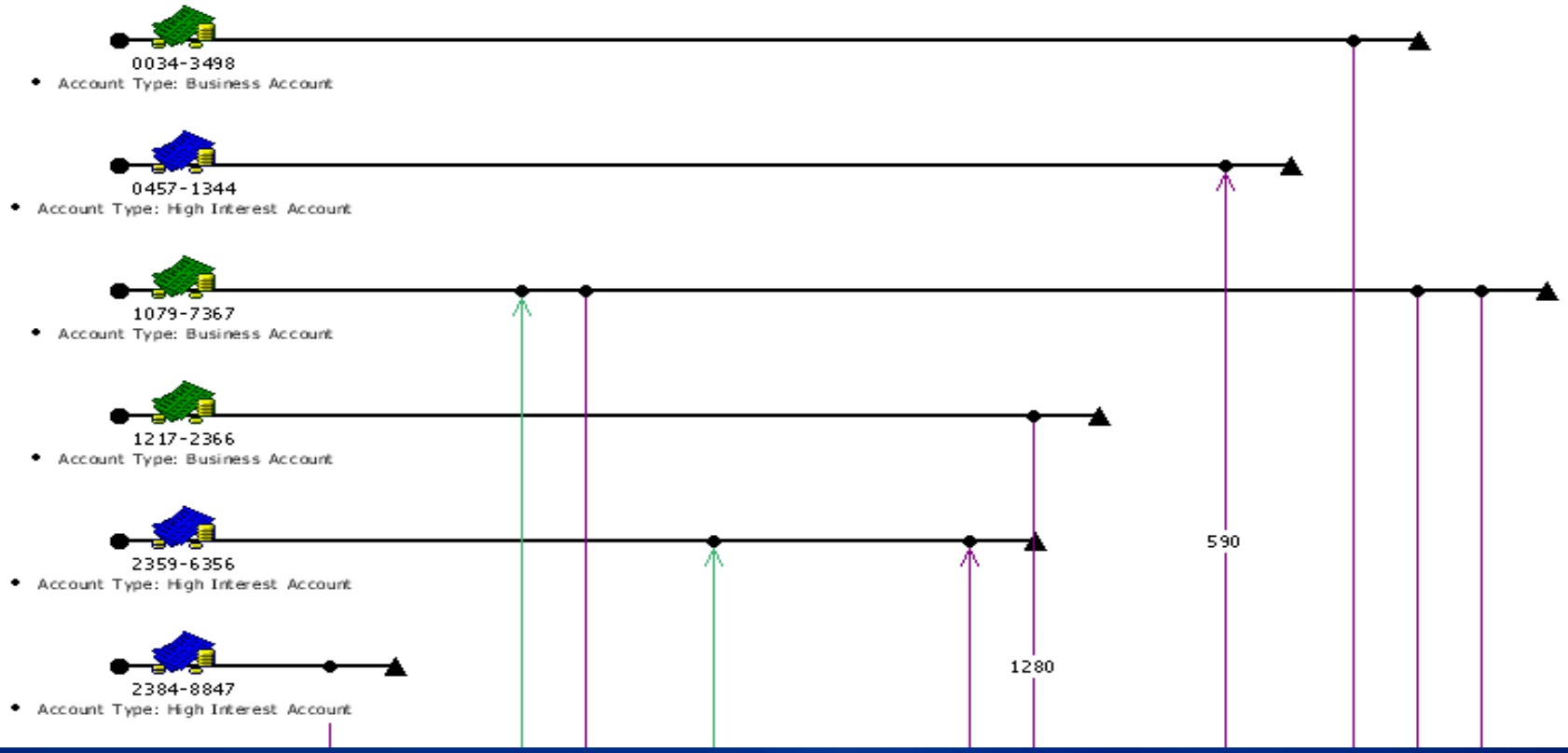
- tranzakciók
- megfigyelések
- időrendek
- kapcsolati hálók
- tulajdonosi viszonyok

Vizualizálás

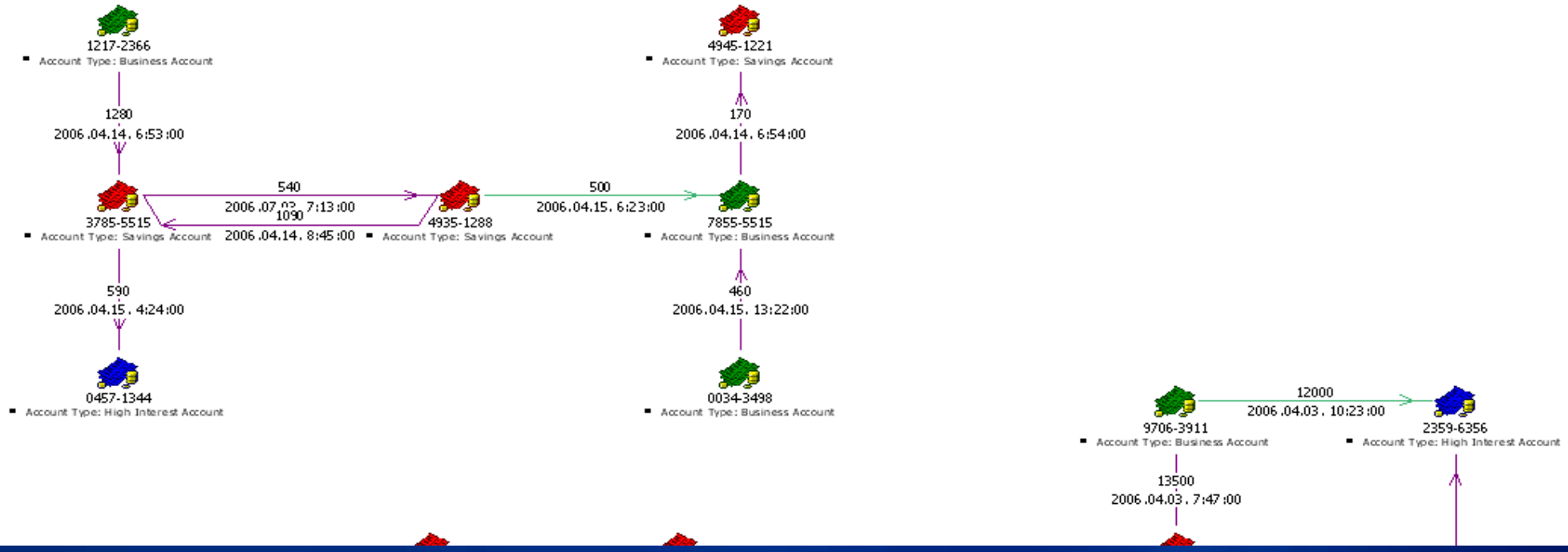
- rejtett összefüggések felderítése
- különböző nézetek

Példa: i2

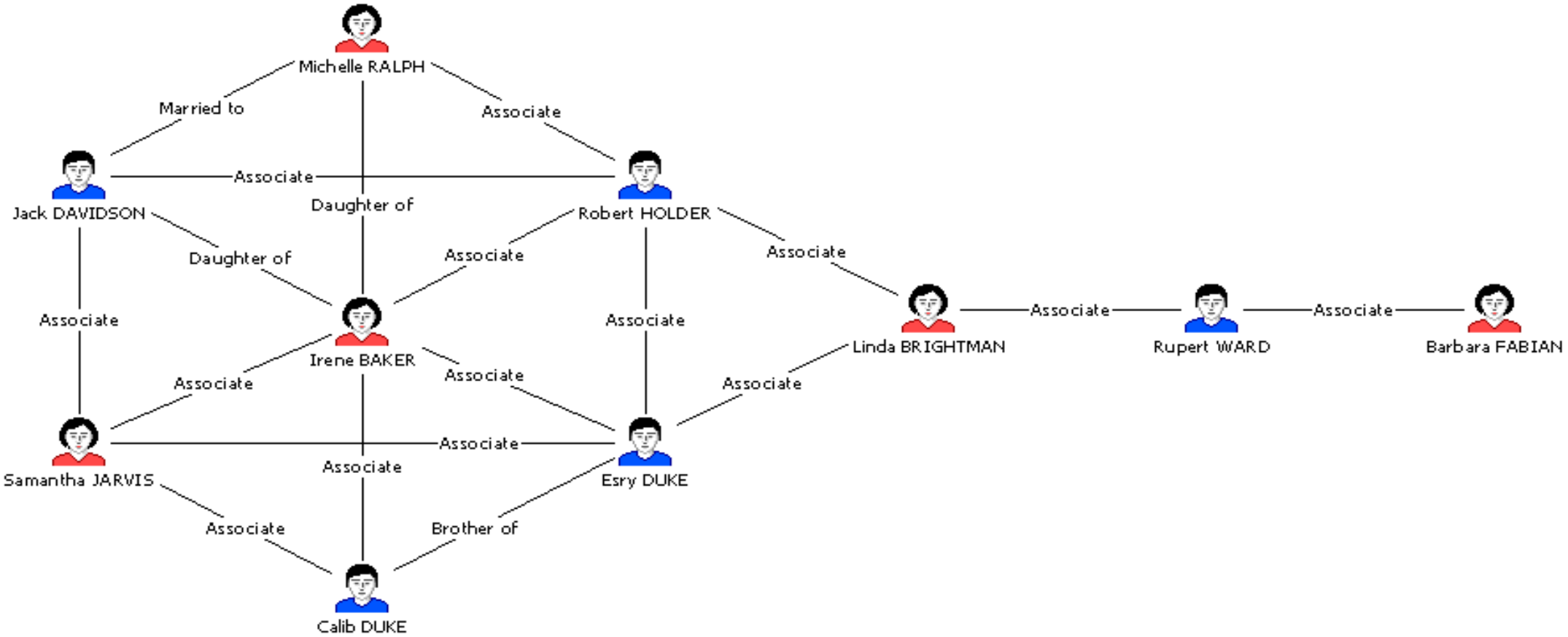
Fraud tranzakciós időrend



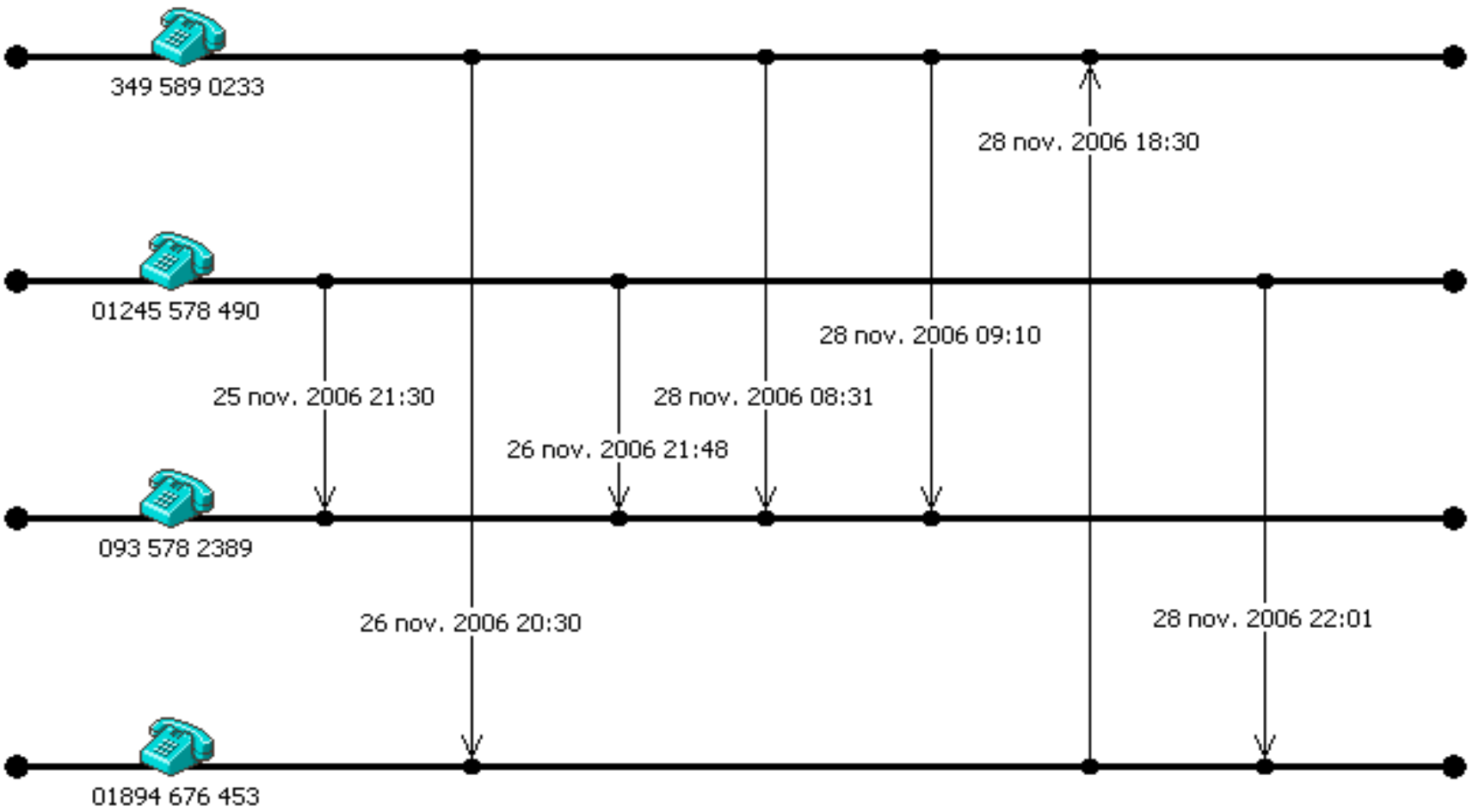
Fraud tranzakció összefüggések



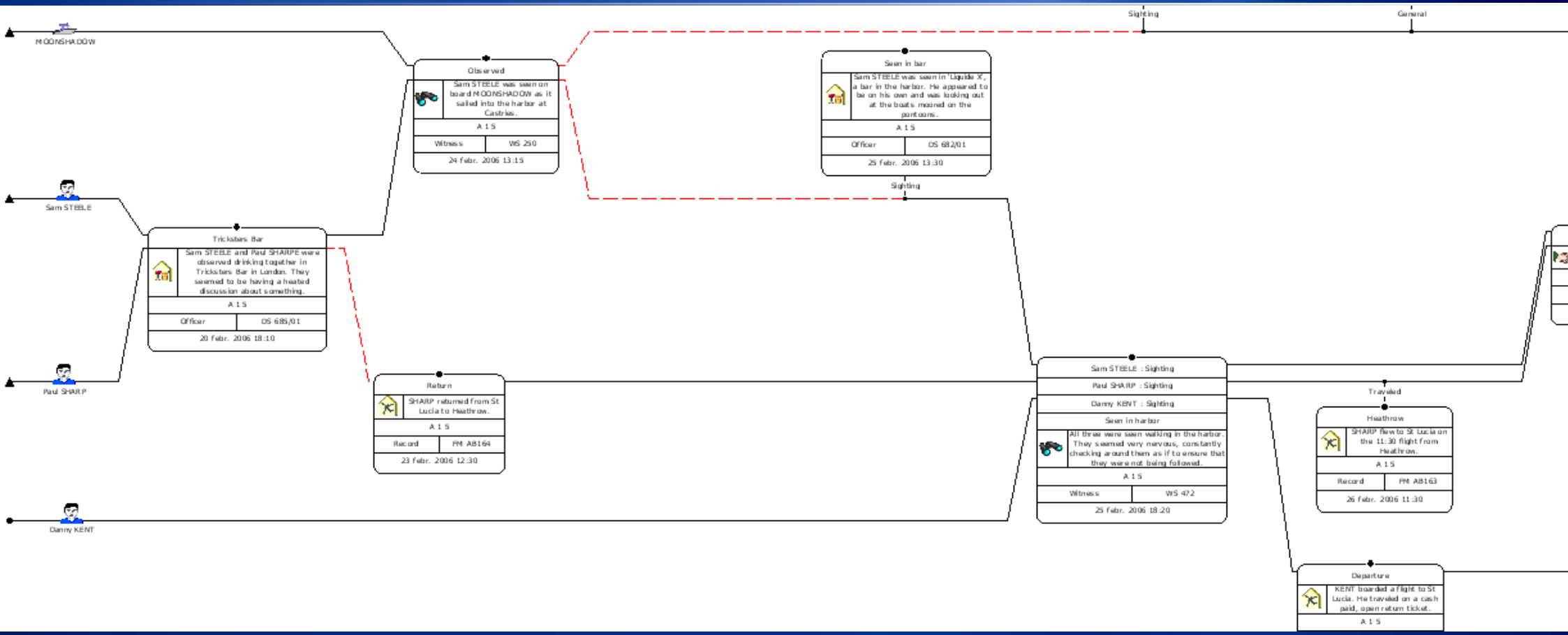
Fraud kapcsolati háló



Telefonbeszélgetések időrendje



Komplex eseménysor



Tranzakció az ügyfél számlája feletti rendelkezés átvételével

“Facility takeover fraud”

Probléma: T-PIN alapú ügyfél-azonosítás. Ezek a legtöbb esetben 4 karakterűek, amikből a híváskor kérésre kettőt mond be az ügyfél telefonon a bankárnak. Mivel a beszélgetések rögzítettek, az a személy, akinek joga van a visszahallgatáshoz, 2-3 beszélgetés alapján ki tudja deríteni a titkos kódot, és az ügyfél nevében ő, vagy valamelyik bűntársa be tud jelentkezni és műveleteket végrehajtani.

Megoldás:

- Szigorú kontroll a visszahallgatási jogosultságokon egy automatizált szoftver segítségével. Ennek garantálnia kell a „maker/checker” funkcionalitást.
- Vezetők havi nyilatkoztatása a hozzáférés szükségességéről.
- A visszahallgatások naplózása, a visszahallgatott beszélgetés tárgyának összehasonlítása a visszahallgató személy feladatkörével.
- Csapda állítása. A csapda elektronikusan naplózott kell legyen, hogy a bizonyítékok tényszerűek legyenek és az eset teljes felderítése az elkövető tudta nélkül történhessen.

Túlzott belső adatközlés miatt bekövetkező csalárd tranzakció

Probléma: A bankok nagy része nem titkosítja az ügyféladatokat típusonként (masking). Azok az intézetek, akik mégis követik a maskingot, elkövethetik a hibát, hogy a batch riportban mégis egyben jelenítenek meg mindent (tehát hozzáférhetővé válik az éles rendszerben hatékonyan letiltott adatállomány).

Példa: Az ügyfél visszaélés miatt letiltotta a kártyáját. Az ügyintéző újat generált neki a rendszerben. Az újonnan generált kártyaszám máris látható lett szinte minden osztály számára (a bank rendszereiben) rengeteg további ügyfél-adattal együtt. Csupán 30 perc telt el az új kártya számának generálását követően és máris telefonált valaki aktiválni a kártyát. A sikeres aktiválást követően az elkövető használta is azt. Az ügyfél biztosan nem tudhatta a számot.

Megoldás:

- Szigorú adathozzáférési kontroll bevezetése (adatkategóriák felállításával)
- Az alkalmazottak által lehívott ügyfélanyagok rendszeres ellenőrzése, és összevetése azzal, hogy eljárásuk szükséges volt-e

Nagy összegű készpénz tranzakciók utáni támadások

Probléma: Bankfiókok kapcsán kétségbeejtő tendencia volt korábban az ügyfelek kirablási esetszámának növekedése. (Az esetek nem szűntek meg teljesen.)
A módszer egyszerű: Az ügyfélnek a nagyobb összegű készpénz felvételeit előre jeleznie kell a fióknak, általában egy nappal a tranzakció végrehajtása előtt. Az ügyfél által leadott kérelem több kézen megy keresztül. Az elkövetőket az egyik banki alkalmazott értesíti az ügyfél személyleírásával (amely kikövetkeztethető a személyes adatokból), a fiók címével, és a várható érkezési időponttal egyetemben. Az ügyfelet a fiók közelében várják már az elkövetők, és mivel a tranzakciót néhány perce hajtotta végre, biztosan nála találják a készpénzt.

Megoldás:

- Az adatokhoz hozzáférő érintettek körének lényeges szűkítése
- Zárt kommunikációs rendszer kidolgozása a nagy összegű készpénz felvételek bejelentésének kezelése érdekében.

Elmaradó törlesztő részlet tranzakciók

Probléma: A banki területek közül az egyik legkevésbé ellenőrzött a behajtási terület. Nagy a fluktuáció és az alkalmazottak jó része szűretlenül özönlik a szabad pozíciókba. Az álláskereső portálok is szüntelenül hirdetik a szabad „collector” állásokat. A 10%-os munkanélküliség ellenére is állandóan van legalább 3-4 cégnél (beleértve a pénzintézeteket is) szabad pozíció. A felvett collectorok munkája nincsen megfelelően kontrollálva: a beszélgetések általában rögzítetlenek, nem ellenőrzik az ügyfelekkel történt megállapodásaikat / ügyfeleknek adott engedményeiket / valóban egyeztettek-e az ügyféllel. Egyes alkalmazottak anyagi ellenszolgáltatás ellenében biztosítják ügyfeleknek a „végtelen” tartozás lehetőségét. Mivel nincs kontrollálva az általuk végzett rendszerbeli utasítás, bármilyen megállapodást rögzíthetnek úgy, hogy ne jelenjen meg a végrehajtandó tartozások között.

Megoldás:

- Szoftveres ellenőrzés (monitoring) a beregisztrált megállapodásokon, és az életszerűtlen szituációk beparaméterezésével napi riasztások küldése

Field Collection csalások

Probléma: Gyakran a „field collectorok” csalnak az útiköltség elszámolással. Első hallásra nem tűnik komoly veszteségnek, de az elcsalt összeg alkalmazottanként havi többszázezer forintot is kitehet úgy, hogy eközben a beregisztrált ügyfél (akire hivatkozva a megtett út el lett számolva) meg sincs látogatva. Mivel nincs ezeken megfelelő kontroll szinte sehol (sem a behajtási vezetők, sem a belső ellenőrök által), a semmi után fizeti meg a bank a tanulópénzt két helyen is: 1. fel nem keresett ügyfelek behajthatatlan adósságai, 2. a behajtók által elcsalt pénz.

Megoldás:

- A legegyszerűbb egy GPS alapú nyomon-követési (és akár központi irányítási rendszert) létrehozni a folyamatos kontroll biztosítása érdekében.
- Adatelemzés és gyanús esetben fizikai követés, megfigyelés
- „Mystery shopping”

Értékesítési ügynökségek felé irányuló tranzakciók

Probléma: Az értékesítést egyre több bank szervezi ki. A belső ellenőrzési munkatársak ritkán veszik észre, hogy a külsős cégek mögött sokszor volt banki alkalmazottak állnak, és így viszik ki a bankból a pénzt. Például, bizonyos Marketing / Sales munkatársak még banki alkalmazottként megalapítják a saját cégüket, használják a bank infrastruktúráját a cég beindításához, munkaidőben menedzselik azt, majd miután beindult, ledelegálják maguknak a sales tevékenységet, és felmondanak a banknál. Az esetek többségében az elkövetőknek továbbra is maradnak kapcsolatai a pénzintézetnél, akik folyamatosan látják el őket információval, de jellemzően az indításhoz szükséges teljes banki ügyféladatbázist magukkal viszik (ellopják).

Megoldás:

•A due diligence folyamat egy része automatizálható lenne. Ennek az egyik legfontosabb része a CI, azaz beazonosítani, mely cég mögött ki áll. Ezt kombinálni lehetne egy rendszeres email és telefonforgalom ellenőrzéssel.

Ügynökök felé irányuló jutalék tranzakciók

Probléma: A társaságok gyakran kevéssé kontrolláltan fizetnek ki új szerződések után jutalékokat. Az üzletkötők nagyobb jutalék reményében egymásnak adogatják át az üzleteket, hogy egy meghirdetett verseny kapcsán az évek óta rosszul teljesítő ügynöknek rekord eredményei lehessenek, vagy azért, hogy a legmagasabb díjazású kolléga részére fizessen a társaság jutalékot. Ez több helyen is fájdalmas:

1. valós teljesítés nélküli kifizetések
2. túlfizetések
3. nem megfelelően nő az ügyfél-portfólió

Megoldás:

- A jutalék elszámolást automatizáltan végrehajtó rendszer kifejlesztése, amely tartalmazza azokat a paramétereket, melyek az ügynökök csalárd szándékú megmozdulásait ki tudják szűrni

Scoring csalással végrehajtott hitelezési tranzakciók

Probléma: A scoring alapú elbírálási rendszerek nem feltétlenül rendelkeznek megfelelő kontrollkörnyezettel, vagy szoftveres támogatással. Ezért sok scoring rendszer viszonylag könnyen feltérképezhető, a beépített szempontok kitalálhatók. Ez alapján az ügynökök máris tudják, hogy hova mit írassanak az ügyféllel. Ez súlyos következményekkel járhat, hisz komoly mértékben növeli a behajthatatlan követeléseket (hitelezési veszteség), a megvezetett ügyfél pedig feketelistára kerülhet.

Megoldás:

•Automatizált elbírálási rendszer kifejlesztése, amelyben az újabb és újabb credit / fraud memok alapján online lehet a paramétereket változtatni. Emellett a rendszer üzletkötők szerinti bontásban figyeli a gyanús „kilengéseket”, ami arra utal, hogy az ügynök egy feltérképezett scoring szisztémához igazodva próbál igényléseket beküldeni.

Összefoglalás

- A csalási esetek 88%-ban volt belső komponens
- A belső ellenőrök és külső auditorok nem a legalkalmasabbak a csalások felderítésére – ennek számos oka van
- A forensic auditor nem bánja, ha gyűlölik – csak derüljön ki az igazság
- A specializált IT támogatás elengedhetetlen a hatékony munkához

Az előadó elérhetősége

Gaidosch Tamás

KPMG Tanácsadó Kft.

tamas.gaidosch@kpmg.hu

887-7139

www.kpmg.hu