Fraud Risk Management

Welcome All

Yes, fraud is a serious subject but in reality it is fun and interesting, both for the investigator & fraudsters, like a chess game.

I can only make this fraud session interesting by using few case studies; videos and by splitting the session to 4 modules stitched nicely for easy understanding.

Logistics for this webinar & Disclaimer

- **Reminder:** During my talk, on & off I will be touching few basic concepts for the students to understand better. Our experienced members and Subject Matter Experts SMEs, are well versed on fraud basics. Appreciate if you could bear these basics in the larger interest.

- **Disclaimer & Acknowledgement**: Case studies; images and Videos here are presented for education and better understanding only. We acknowledge sincere thanks to each of the references covered in this presentation. These are NOT FOR ADVERTISEMENT For security reasons names are changed.

- Let us take a deep dive into our Fraud Risk Management session right away - **4 module structure.**

Do you like challenges – become a CFE

Fraud Risk Management (FRM)

A monster concept - Bite size for you…. into 4 modules

Module 1
Fraud risk management program
Concept and Accountability

Module 2
Banking fraud

Module 3
Digital fraud & on-line
Internet of Things IoT

Module 4
FRM Tools & Global scenario
AI, ML, Data Mining, CAATs

Module 1 – Fraud Risk Management Program

1.0 Concept Overview

- Fraud
- Risk
- Management of Fraud Risk

2.0 Effective fraud risk management program

- Industry and company specific
- Organization size
- Complexities recognizing inherent risks & systemic risks.
- Bank fraud & Digital fraud focused

3.0 Accountability

- Statutory Auditor or IA or Top Management or who else?
- Board Room to Mail Room + key role of Internal Auditor
- AML investigation – (Case study: CID interaction - FAX tapping)

1.0 Concept Overview – Fraud, Risk, Management of Fraud Risk

Error vs Fraud

- Error can be accidental, but there can be NO accidental fraud
- Origin of the term “Fraud” - **F**inancial **R**eward **A**cquired **U**nder **D**eception
- **Deception** is intentional - made for personal gain or - to damage another individual
- Deliberately deceiving another - in order to damage them - to obtain property or services unjustly
- In criminal law, **fraud is a crime or offense**

Internal vs External fraud

Internal: Occupational / Employee fraud; corruption, asset misappropriation, & financial statement fraud. Not charging friends & family.

External: Risk of unexpected loss perpetrated by persons external to the organization – this can be financial loss; material or reputational loss.

Threat – unintentional vs intentional

- A **threat** is what we're trying to protect against. A staff mistakenly accessing wrong info in the system; A disgruntled staff accessing the same system to inject virus or add spyware, malware it is intentional threat. Risk is high in case of Intentional threat.

1.0 Concept Overview – Risk and Emerging Risk

Risk

- The potential for loss of life or money or damage as a result of a **threat,** exploiting a vulnerability.
- **Risk** is the intersection of assets, **threats**, and vulnerabilities.
- **Types of Risks include:** Inherent risk; Systemic risk; Reputation risk, Regulatory risk; Transaction risk; Employee fraud risk (occupational fraud)

FRAUD is a Risk - Fraud risk is the risk of various types of fraud, a Co could face from internal and/or external.

Emerging Risk: High risk of uncertainty - no clue; no basic information; can't even assess the frequency & severity of a given risk. Emerging risk is completely a beast, never experienced before but causes havoc. Best example, right now in 2020 world is facing this, Emerging Risk **"Contagion"** movie released in 2011. **VIDEO** **https://youtu.be/VZGHGVledzA**

Laurie Garret wrote a book in 1994 "The coming Plague" reported on multiple pandemics. Says Contagion as Partly fantasy part reality and totally possible Emerging risks in banking: Security breaches /New Regulation on data & security SWIFT.

RISK ASSESSMENT – Banking health

RISK – Heat Map – covered in Banking fraud - AML Risk heat map in tools - STRESS TEST - As a banking regulator in Middle East (pro-active real estate market) & in Canada, we used multiple tools for risk assessment

1.0 Concept Overview: Fraud Risk Identification Process

The **fraud risk** identification process should include:

- Assessment of the incentives,
- Pressures
- Opportunities to commit fraud
- Intention

Along with pressure and opportunity, fuel for committing fraud is complete with rationalization.

Opportunities to commit **fraud** exist throughout any organization and it is HUGE in banking and digital environment. Imagine if there is lax in internal controls and a lack of segregation of duties, it is a field day for fraudsters.

Case study: Over reliance of branch manager on a shrewd staff. Unreconciled demand draft A/c - DD issued without consideration using client A/cs & customer cash was siphoned off with false entry in passbook only. Branch control returns fudged.

2.0 Effective Fraud Risk Management

Product & its nature: (high potential for fraud)

- Gold & bullion business / Cash business / Ease of resale

Factors to Consider for an Effective FRM

- Conducive to fraudsters
- Access ; Accounts;
- documentation;
- oversight; related party deals;
- time off access;
- more complex process high potential for fraud;

- Weak Board of Directors -strong case for fraud
- Soft touch
- Attrition rate
- Weak internal audit function - fertile for fraud
- Pressure: Dissatisfaction; classified info; market expectation; avoid invoking BGs

<u>Case study</u>: Feel of segregation on books - case study: spurious gold Aged supervisor reliance on joint custodian.

Internal auditor role is very critical, on the ground, during audit: PIN & CARD segregation /eyes & ears open / faulty cash counting machine.

3.0 Accountability

Who on earth is accountable? Is it Statutory Auditor or Internal Auditor or Senior Management ?

- Board Room to Mail Room & key role of Internal Auditor. Limited extent Statutory too

- “Does “one size fits for all” FRM model apply? **BIG NO** - Customization is key.

- In ensuring effectiveness of FRM program, Internal Auditor does play a big role in ensuring strict compliance of following ACFE guidelines

- FRM depends on the company size; complexity and industry fitment. Vulnerability
- Risk tolerance – there is tolerance level for risk but for fraud – zero tolerance (Tone at the Top is critical)

3.0 Accountability (Contd.)

Key elements to be present in the Fraud Risk Management documentation & Org. structure:

• Roles and responsibilities - Board & Senior Management • Commitment - Tone at the Top • Fraud awareness (training / webinar) • Conflict disclosure • Detailed Fraud risk assessment • Emerging Risk radar • Reporting protocol – follow up action	• Red flag • Whistleblower protection • Investigation process documented • Corrective action & serious penalty • Quality assurance at each stage • Continuous monitoring • Eyes & Ears (experience need not be yours) • Dynamic & not static (Example COVID frauds)

World is Changing, so as Rules

Module 2: Banking Fraud

- **Fraud toes the dotted line of money**
- **Money = Banking, Banking = Fertile ground for Fraud**

Topics Covered

- Anti Money Laundering – AML
- Very High Risk cases lead to potential fraud - equally important
- International Case Studies – Risk Assessment / Credit & Gold Bullion /Large Scale
- Retail Banking – Fighting Financial Fraud – Canadian Bank
- Bank Fraud – Root Cause Analysis (RCA) is critical. Not to repeat.
- Your own history is important, but experience of others is more important, to learn from - to pro actively arrest fraud.

Bank Fraud – AML

- **Money laundering occurs when transferring money across borders**
- **Major customers of money laundering are:**
  - Tax evaders
  - Drug dealers
  - Terrorist operators

- **Among others, 2 key factors that affect the risk of an a/c**
  - Country risk: Destination
  - Transaction risk: Volume, frequency

Case studies… Very High Risk just stops large fraud / AML

Case Study 1: Gold & Bullion – VH Risk Rating International

Case Study 2: Internal Controls – Fraudulent fund transfer - International

Video on Retail Banking – Fighting Financial Fraud – Canadian Bank
https://globalnews.ca/video/5040683/fighting-financial-fraud

Case Study 3: Anti Money Laundering (AML) Tracing final Account – International

Case Study 4: Regulatory review – credit portfolio - risk downgraded – International

Case study Summary … Bank fraud

Root Cause Analysis and CAATS: Common responses – accountability haunts again

- Top Management -no clue on how it happened
- Statutory auditor: off the hook due to " off the books" concept
- Accountability – Zero
- Internal controls – All in one place – controls on the air
- Controlling / monitoring authorities

- Extremely serious – calls for severe action
- Systemic issue – responsibility lies from Big picture principle – still accountable
- Extremely critical – to be booked
- Lack of segregation – too much reliance on single individual
- Equally responsible and accountable
- ***Lots of resemblance to our Punjab National Bank & Harshad Metha fraud cases***

Module 3 – Digital Fraud and Online

- With convenience, comes risk.
- As payments move online, fraudsters follow closely.

Topics Covered

- **Smart Phone – virus & take over, On-line frauds**
- **Internet of Things (IoT)**
- **Artificial Intelligence (AI) -** area of computer science that emphasizes the creation of intelligent machines that work and react like humans

DIGITAL Fraud – Internet of Things IoT

In simple terms IoT is the network of physical devices, home appliances etc, embedded with electronics, SW, sensors and internet connectivity (web enabled) which enables these to connect, collect and exchange data. **DOWNSIDE: Security concerns; insecure small gadgets / gaming console in market, opens the flood gates to fraudsters.**

IoT EVERYWHERE - Smart phone, Internet, IoT whatever gadget you touch, there is convenience tagged to potential fraud!! With Corona we are more desperate for convenience. As living with convenience is a necessity going forward, learn how to embrace this risk & lead a lifestyle.

IoT is everywhere – smart phone/appliances/security system/ Fitbit / Scale / Sleep machine / TESLA - Fear not, it is not Digital pandemic. Example: TESLA / Weighing scale / Sleep machine. **For you, on-hand basic solution to mitigate Digital Risk – AAA A**wareness ; **A**daptability; **A**lertness with common sense. Technology can be like junk food. We will consume it even when we know it is bad for us.

On-line Fraud - As payments move online, fraudsters follow closely.

Global ecommerce market is predicted to grow to USD 5 Trn. in 2022 and 20 % of global consumer sales will be online. Fraud loss is estimated to be 1.8% of online sales. Digital revolution overturned the Fraud dynamix to a new level.

DIGITAL Fraud Mitigation – Cybersecurity technology

Strike a right balance between cybersecurity technology against your security policy needs.

Major trends: biometrics, mobile authentication, and risk-based authentication.
AI application, a major mitigation tool

Biometric – users feel & user pattern is key

- Fingerprints / Pattern matching;
- Facial-Identification and measurement of points on the face.
- Voice recognition-Voiceprint ;
- Retina Iris recognition;
- Behavioral biometrics: Using subtle factors like typing style, swipes on a mobile device, dwell time, and technical identification.

DIGITAL Fraud Mitigation – Cybersecurity technology

Mobile authentication:

- Mobile push technology that let you swipe or accept to authorize;
- Built-in mobile biometrics;
- OTP
- Advanced analytics is one of the major solutions

VIDEO - Real time fraud prevention in a real time world

https://www.youtube.com/watch?v=sMDg7ld1tZU&app=desktop

On-line fraud - SWIFT Fraud

SWIFT Fraud - Key findings I have conducted SWIFT controls - submitted Executive Note on Emerging risk, highlighting SWIFT as EMERGING RISK.

•**Under SWIFT South East Asia accounts for** 80% of fraudulent beneficiaries **(Red flag)**

•**USD currency used in 70 %** of attempted thefts - use of Euro **(Red flag)**

•**Sleeper cells** - attackers continue to operate 'silently' for weeks or months after penetrating a target, learning behaviors and patterns before launching an attack.

•**Soft target of unused payment corridors***:* vast majority of fraudulent transactions used payment corridors (combinations of target and beneficiary banks) that had not been used during the previous 24- 36m (**Real time Advanced Analytics AI can solve**)

•**Insider collusion** resulted in the quick identification of financial institutions targeted by cybercriminals – in most cases before attackers were even able to generate fraudulent messages; the exchange of relevant and timely cyber threat intelligence has proved critical in effectively detecting and preventing attacks. **(Basic control lost)**

Module 4 – Fraud Risk Management Tools & Global scenario

- **Create Reporting avenues** – Whistle blower / Sectional reporting like immigration fraud / fraud against elders / Canadian Anti Fraud Center / Canada Border Service Agency for Document fraud / anonymous / community policing / peer audit
- Computer Assisted Auditing Techniques (**CAATs - used for risk based audit too.)**
- AML - Anti Money Laundering – **RISK HEAT MAP**
- Emerging risk Analysis - Predictability
- Artificial Intelligence (AI) – Predictability
- Machine Learning
- Data mining – Big Data
- DATA Analytics

21st century fraud landscape…

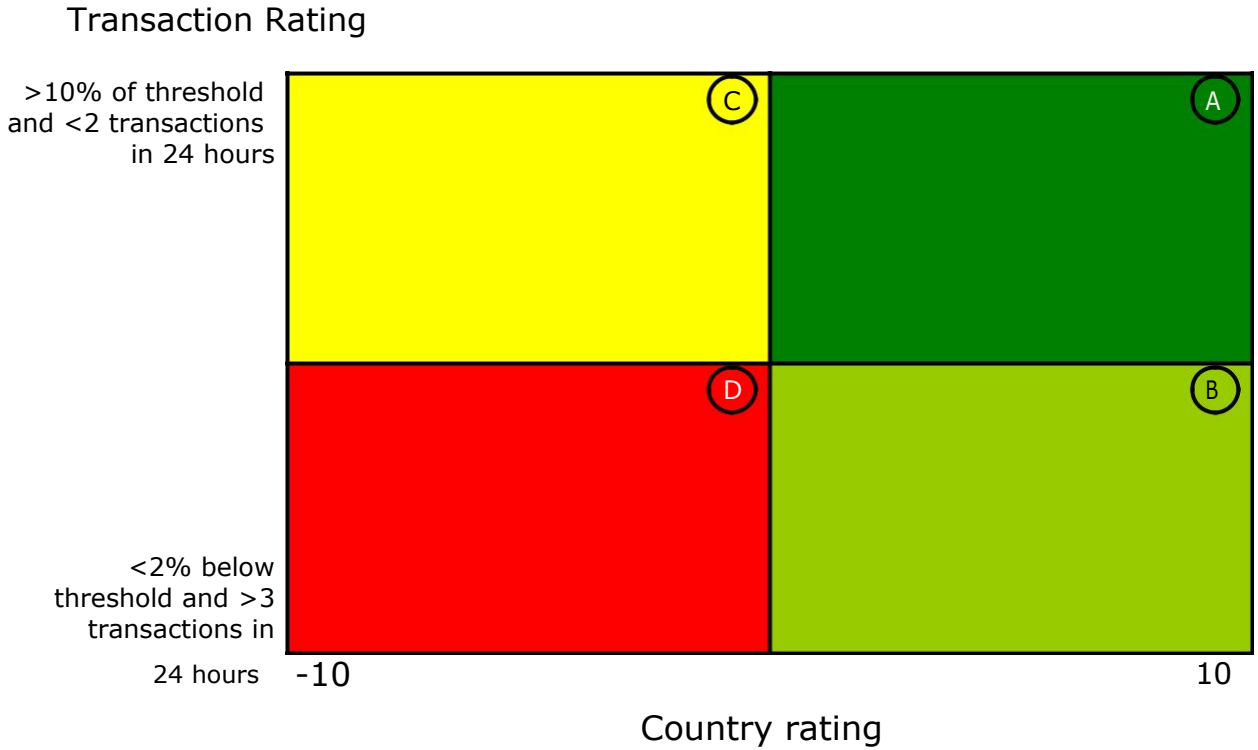
We are in digital school, move to

PREDICT FRAUD

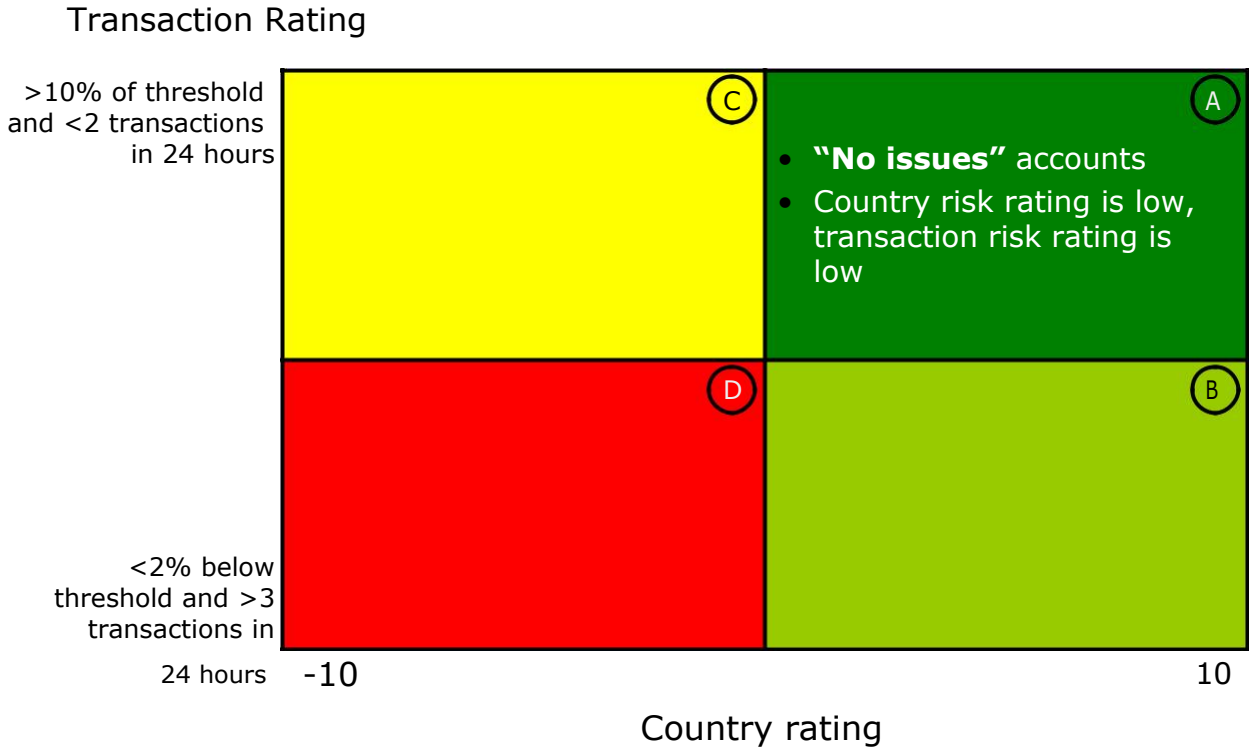
PREVENT FRAUD is traditional, still valid - Old is Gold!!

Risk Heat Map in Anti Money Laundering - AML

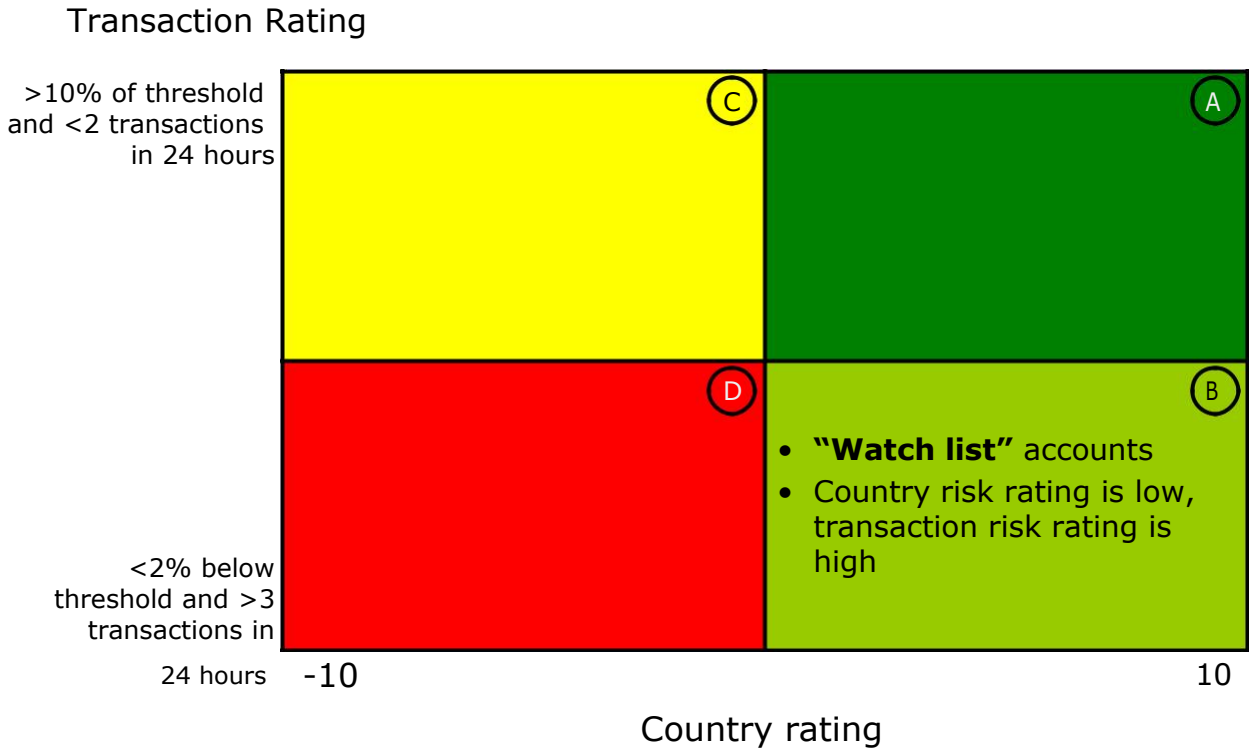
Accounts are plotted on a "risk chart" based on country, transaction risks



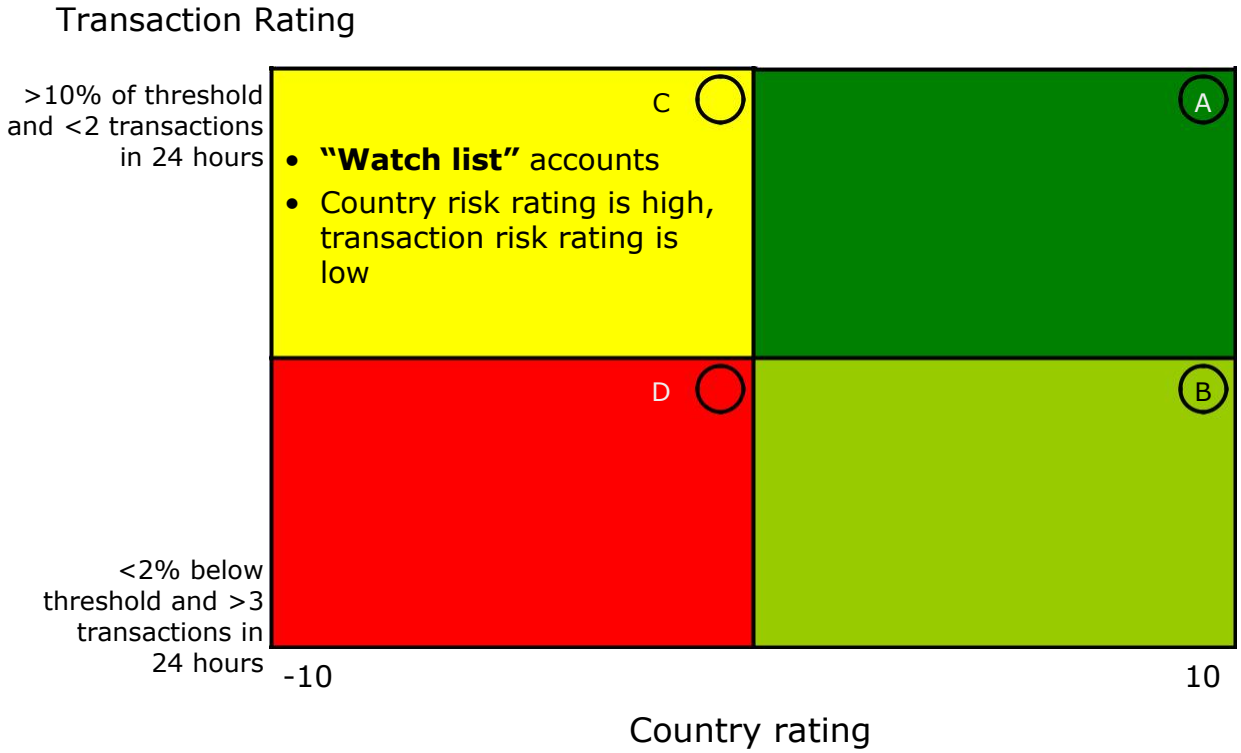
Cool & Green map"Risk chart" based on country, transaction risks



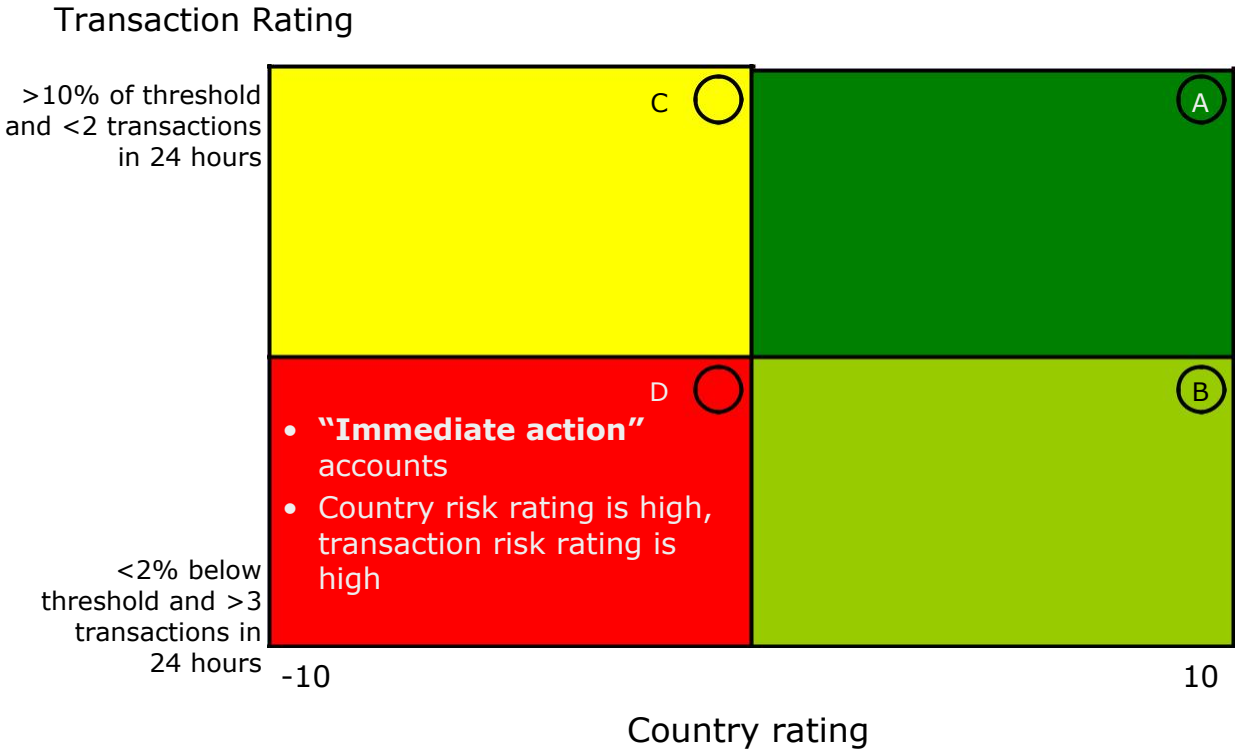
Still cool "risk chart" based on country, transaction risks



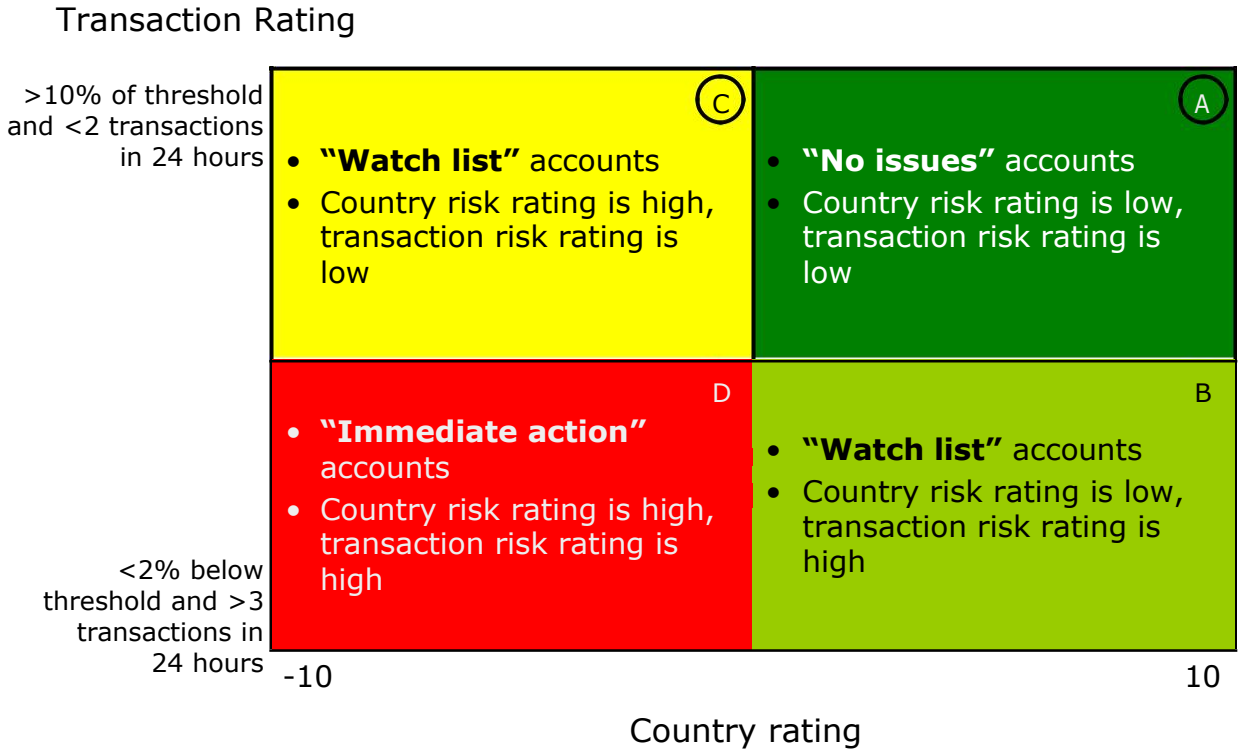
Feeling warm - "risk chart" based on country risk & transaction risks



Hot - Real Heat Map & "risk chart" - Both high risk - country & transactions

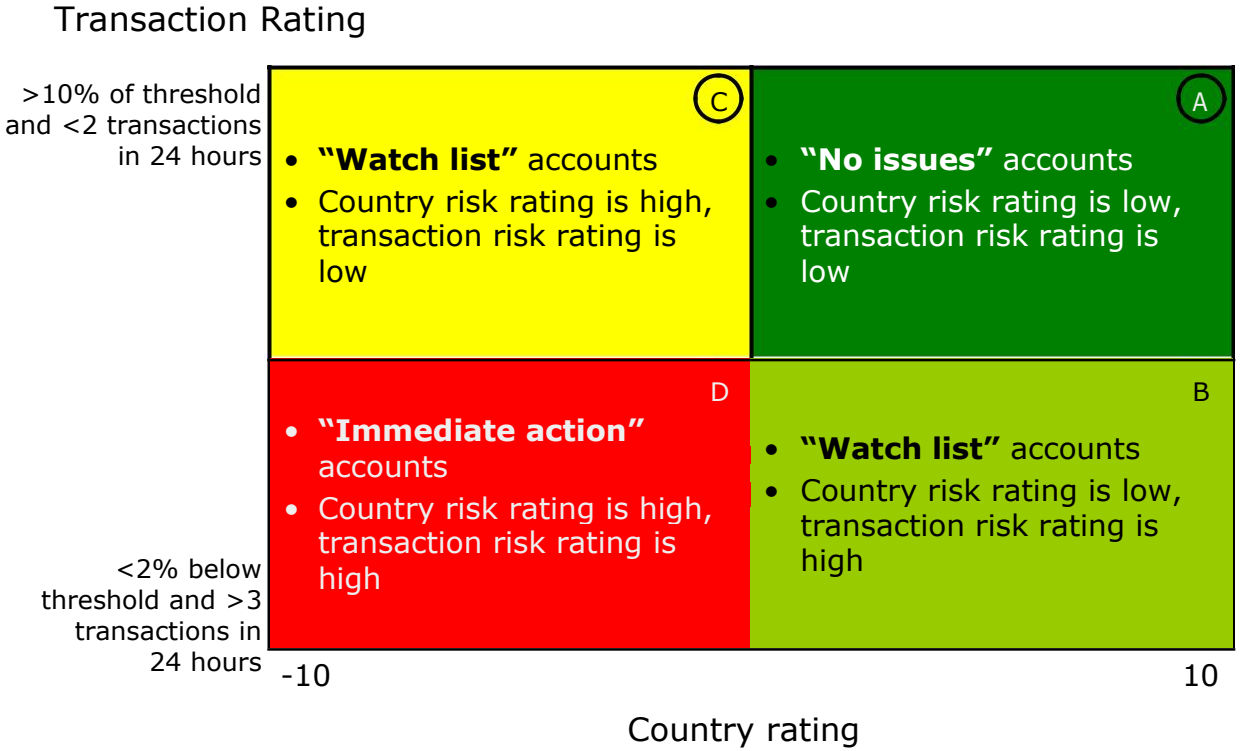


Hot - *Real Heat Map & "risk chart" - Both high risk - country & transactions*



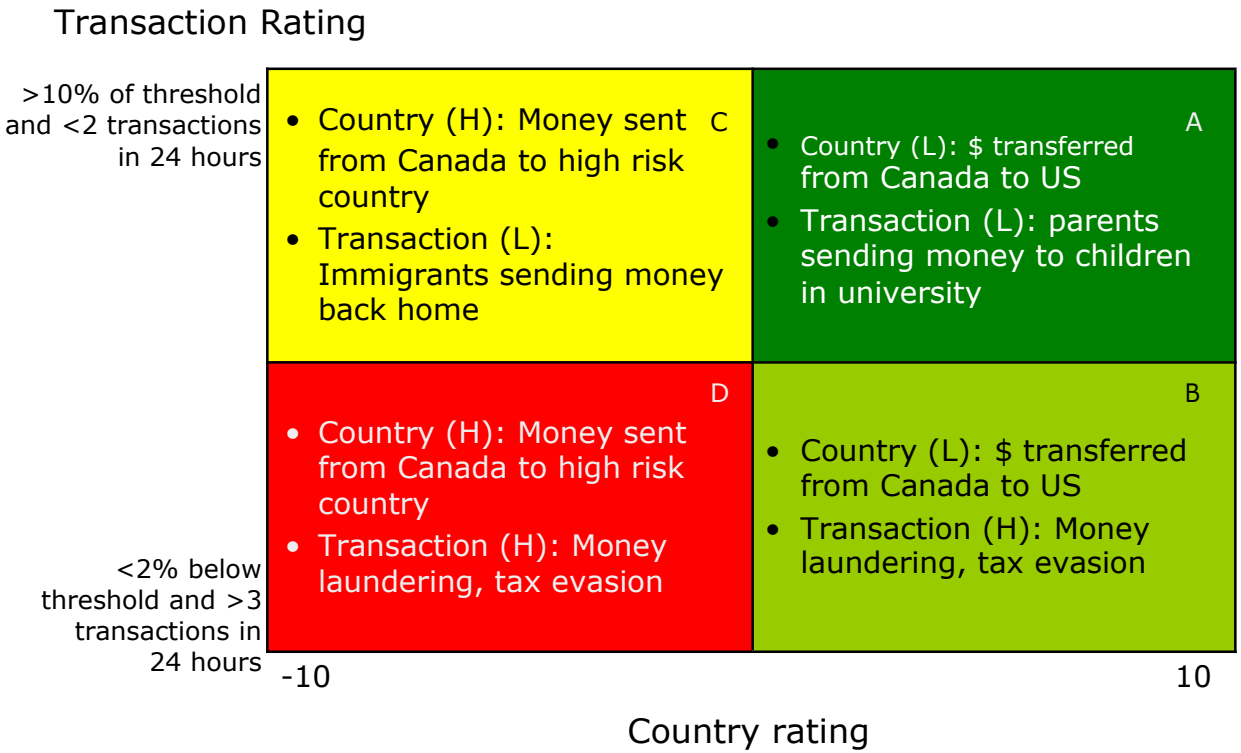
Hot - Real Heat Map & "risk chart" - Both high risk - country & transactions

Each account is plotted on a "Risk Heat Map" based on country risk & transaction risks

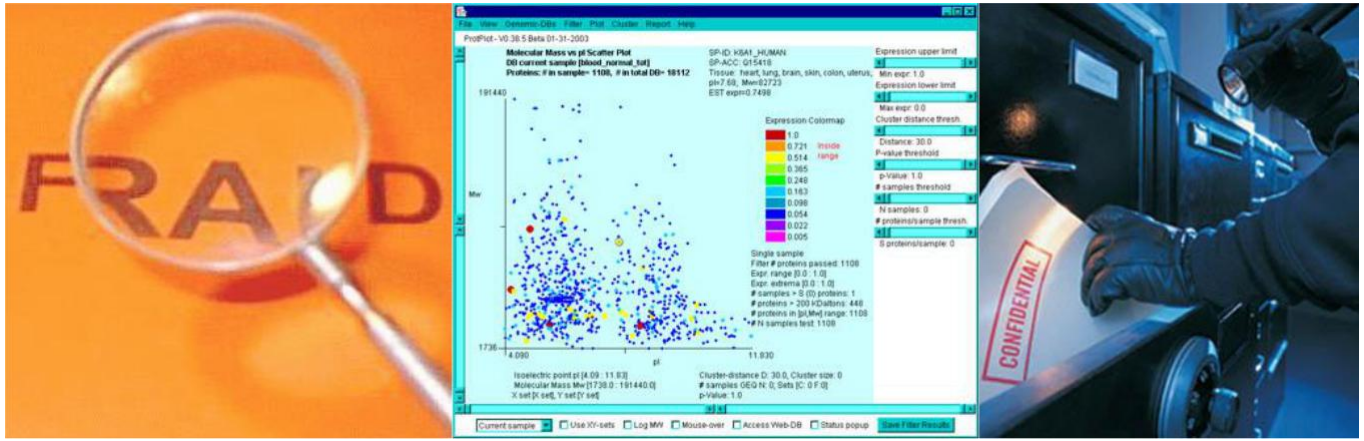


Hot - *Real Heat Map & "risk chart" - Both high risk - country & transactions*

Account examples that might fall under each quadrant



FRM Tools - DATA MINING & CAATs



Data Mining is torturing the data until it confesses.
It is a process and a valuable **tool** as well. Collects **volumes of data** with the objective of: finding hidden patterns and analyzing relationships between numerous types of data developing predictive models (process by which a model is created to try to best predict the probability of an outcome)

Computer Assisted Auditing Techniques (CAATs)
Powerful tool for fraud prevention and fraud detection & in risk based internal audit too.

FRM Tools - Artificial Intelligence (AI) & Machine learning (ML)

AI in simple terms – to create technology that allows computers to function in a more intelligent manner – simulating or creating intelligence – **trying** to replace humans. More useful in repetitive jobs and basic problem solving tasks and where predictability is involved

Machine Learning: ML is a form of AI that enables a system to learn from Data. Types of ML: Supervised learning teaching AI with supervision; Learn from Surroundings; Unsupervised learning

- **AI & ML APPLICATION** in online mobile cheque deposit of cheques – without visiting the branch
- Email category in Gmail like promotional, primary etc done by machine learning
- A I Examples: SIRI / ALEXA / TESLA / AI Auto pilot in commercial flights / Google AI powered predictions / Rideshare APPs use AI to find best & fast route / Spam filter in your email in box is powered by AI / credit decisions in analyzing application details in volume

VIDEO - Let us watch AI in action
https://www.youtube.com/watch?v=0oRVLf16CMU&feature=youtu.be

AI & Machine learning in Fraud radar

- The future of **AI-based fraud prevention** relies on the combination of supervised and unsupervised machine learning.

- **Supervised** machine learning excels at examining events, factors, and trends from the past. Historical data trains supervised machine learning models to find patterns not discernable with rules or predictive analytics.

- **Unsupervised** machine learning is adept at finding anomalies, interrelationships, and valid links between emerging factors and variables.

- **Combining both** unsupervised and supervised machine learning defines the future of AI-based fraud prevention and is the foundation of the top nine ways AI prevents fraud

Artificial Intelligence in Fraud prevention radar

- **Trends and patterns:** AI is re-defining fraud prevention from relying only on past experiences to taking into account emerging activities, behaviors, and trends in transaction anomalies.

- **Fast:** AI's ability to detect fraud attacks in almost real time using advanced AI-based rating technologies like Omniscore is the future of fraud management.

- **Pro-active:** By having an AI-based fraud prevention system do the work of evaluating historical data and anomalies, customer experiences can stay more positive, and the more sophisticated nuanced abuse attacks can be stopped.

- **Minimizing fraud loss:** Provides fraud analysts with real-time risk scores and greater insight into where best to set threshold scores to maximize sales and minimize fraud losses

- **Aids in compliance:** internal business policies regarding the sales of specific products to specific countries based on distribution and reseller agreements.

- **Fraud prevention** Using Neural Networks analyzing frequency / type of transaction / size / kind of retailer involved – throws out exceptions – red flag.

SUMMARY

KEY, PRACTICAL TAKE AWAY FOR YOU - FROM NOW ON

Remember: Where there is money or financial gain, there is fraud. You being a professional is part of the game You can play any role, be a student, Practicing CA or Employed CA, Subject Matter Expert, Board member, Executive, Administrator, Administrative Assistant, Personal Assistant, Mail Room clerk, Businessman MSME or Large .

Individual accountability – it is YOU, tap your forensic brain. be skeptical & be alert.

Keep your eyes and ears open. Report in any form to save your skin and to save your entity and your loved ones; Extreme caution in reporting, submit special reports immediately on High or Very High risk cases without waiting for the audit to complete.

It is time to Predict fraud using evolving technology, while keeping the basics of prevention in tact

Fraud is interesting, as an investigator only!!!