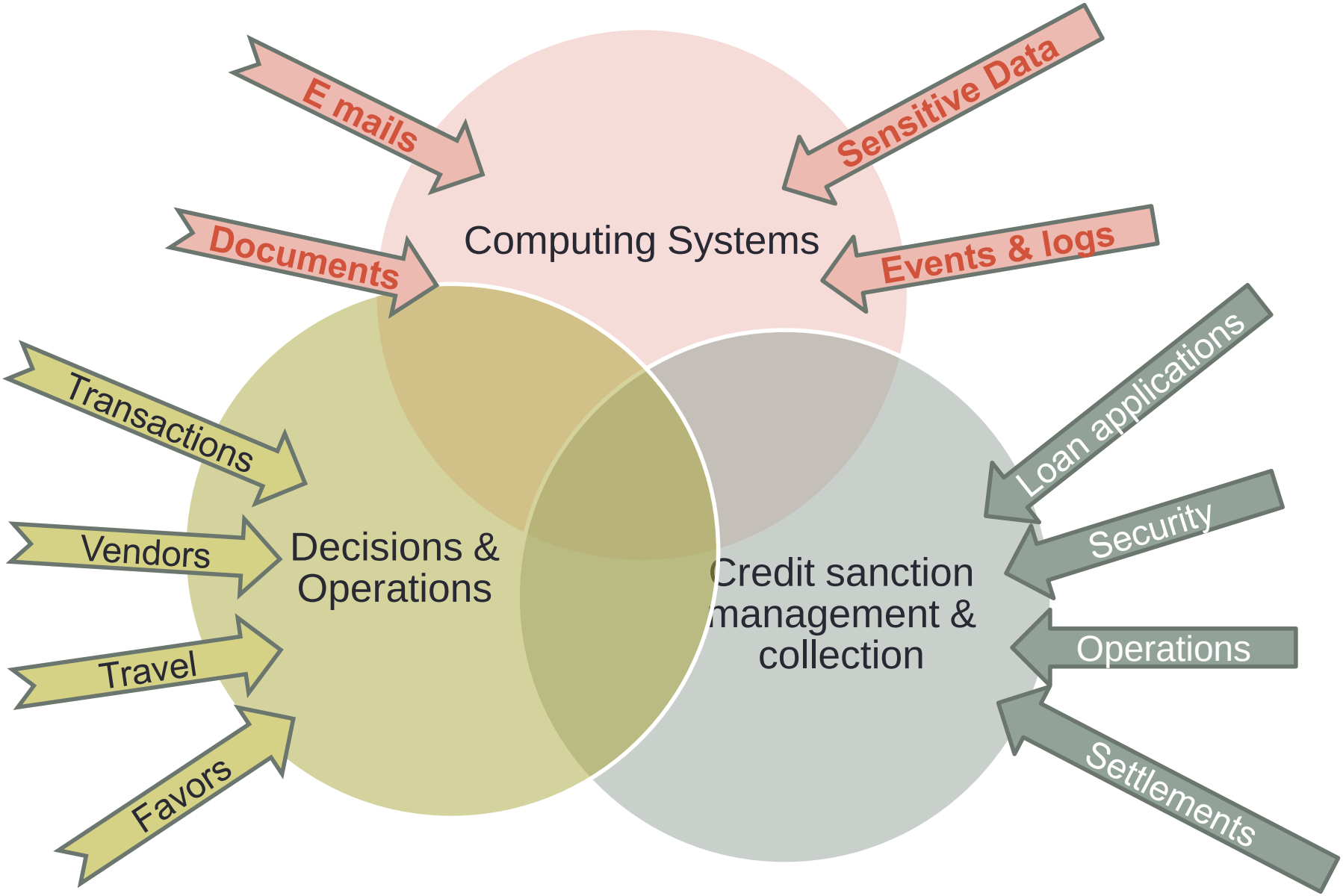
EFFECTIVE USE OF VARIOUS FORENSIC AUDIT TOOLS FOR BANKERS & FINANCIAL INSTITUTIONS WITH LATEST TECHNOLOGIES

By
CA S Santhanakrishnan
Managing Partner, PKF Sridhar & Santhanam
Central Council Member, & Chairman IT Committee ICAI
Chairman, Catholic Syrian Bank

FORENSICS……

BFSI Fraud Domain



Predictive, Preventive and Curative Systems for Fraud Management & Control

Transaction Fraud Monitoring	• **Multi channel multi product fraud monitoring** • **Single Channel (Internet , ATM , Card Fraud etc) monitoring**	✓ Chief Risk Officer / Head – Risk Management ✓ Channel Head (For each individual channel) ✓ Head – Cards Business
Non Transaction based monitoring	• **Internal user monitoring solutions** • **Application fraud monitoring solutions** • **Non Financial Fraud monitoring solutions** • **AML/Ongoing KYC monitoring solutions**	✓ Head – Internal Vigilance ✓ Head – Card/Loans business ✓ Head – Risk Management
Dash boarding solutions	• **Real time dash boarding solutions for vigilance/audit or risk management users** • **Real time dash boarding for branch/regional management users** • **Offline reporting solutions for frauds / vigilance / AML/CDD/KYC**	✓ Head – Risk Management ✓ Head – Branch Banking / Regional head ✓ Head – Risk Management
Customer facing solutions	• **Complex event monitoring and multi channel alerting for specific events (Includes providing a customer front end to define their own criteria)** • **Mobile based purchase controlling solutions (SMITCH)** • **Moments of truth solutions based on pre-defined alerting criteria**	✓ Chief Risk Officer / Head – Risk Management ✓ Channel Head (For each individual channel) ✓ Head – Cards Business

Predictive, Preventive and Curative Systems - Examples

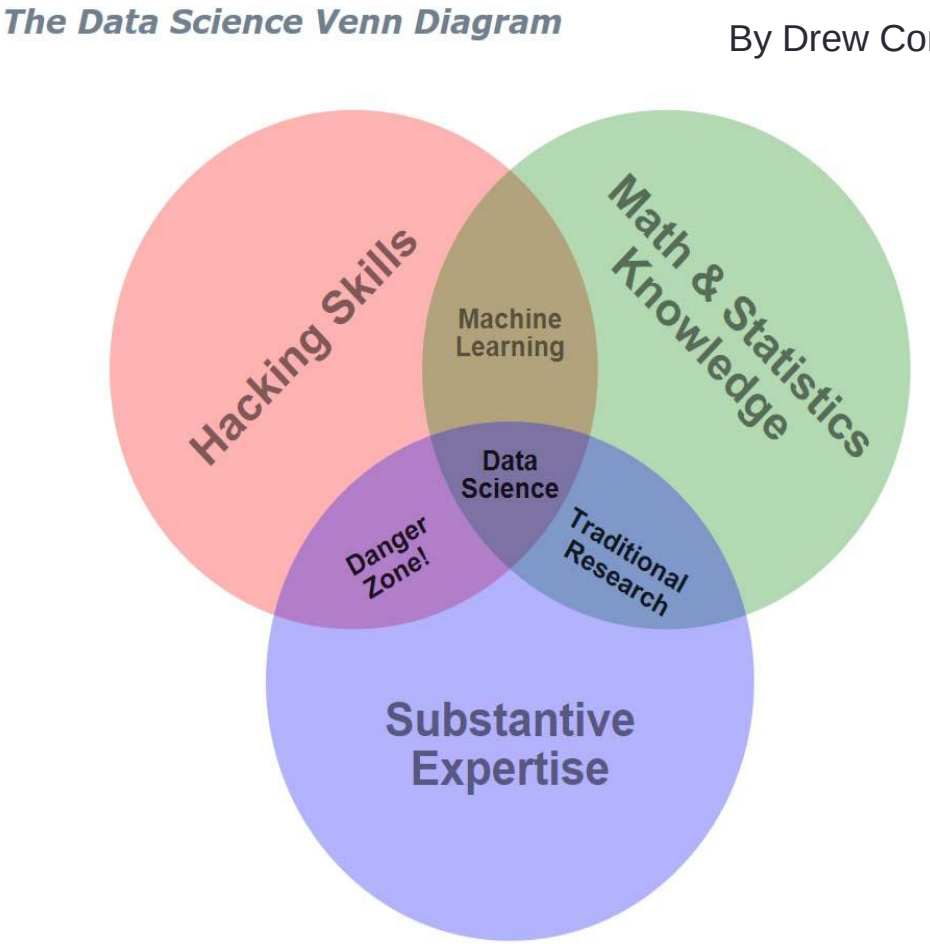
	PREDICTIVE	PREVENTIVE	CURATIVE
Transaction Fraud Monitoring	• Pattern Analysis and alerting	**Stopping the Transactions and alerting**	Risk Analysis and Process change, Provisioning
Non Transaction based monitoring	Network Analysis & Alerting	**Stopping the sanction, recalling the Advance, enforce security etc.,**	Risk Analysis and Process Change, Provisioning
Dash boarding solutions	• **Risk Analytics** • **For Alerts, & Drill down Data** • **Reports and heat maps**	**Approval for suspect Transactions @ higher level**	Risk Analysis & Process Change, Provisioning
Customer facing solutions	• Event Driven Real Time Alerts	Stopping the Transaction, Calling the Customer for Confirmation.,	Event Creation and and risk limit set up etc.,

What is being done now?

WHY	WHAT	HOW
Lack of Regular Monitoring	Continuous Monitoring (Daily / Weekly)	Offsite Monitoring Team to Study patterns & Initiate Corrective actions
Sample Based Monitoring	100% Monitoring	
Discrete Reporting	Consolidated – Risk Based Reporting	Daily Exceptions for Concurrent Auditors – Spot Verification @ Critical Branches / Units
Obsolete Auditing Tools & Techniques	Use of Centralized Monitoring tools and Framework	

DATA …..

What is Data Science and how to marry with Forensics?



Hindsight – Insight – Foresight

- Any analysis follows this progression
- The shorter the gap between the three phases the better
- The faster we get to foresight, the better
- Data Science is Foresight
- Risk Management in banks provides great parallels

A data driven solution keeps the exploiters guessing

Progression of Data Science

Hindsight

- "It is easy to be wise after the event." Arthur Conan Doyle, The Complete Sherlock Holmes
- **In Risk Management:**
  - Began with looking at which transactions, customers seemed risky
  - Interesting exercise but not very useful monetarily

Analysis of drawing over DP

Insight

- " A moment's insight is sometimes worth a life's experience" – Oliver Wendell Holmes Jr.
- **In Risk Management:**
  - Progressed with analyzing what varied with what
  - Insight was useful to understand the difficulty in drawing conclusions

Use this past data to determine pattern

Foresight

- "Business, more than any other occupation, is a continual dealing with the future; it is a continual calculation, an instinctive exercise in foresight" – Henry R. Luce
- **In Risk Management:**
  - Sophisticated artificial intelligence based models introduced
  - Data driven predictions completely revolutionized the art of the possible
  - Need of the hour, to move from Hindsight to insight to Foresight

Send real time alerts when a customer will exceed DP (even without details updated)

What Data Can do to you?

Volume + **Variety** + **Velocity** = **BIG DATA**

- People have been collecting data for a long time but have not always been able to generate value
- Still searching for needles but the haystack is growing exponentially
- More difficult to find needles in the haystack now than before
- Audio / Video / Unstructured / Structured data
- BIG Data can be of value only with DATA SCIENCE

Value = **DATA SCIENCE**

TECHNOLOGY & TOOLS…..

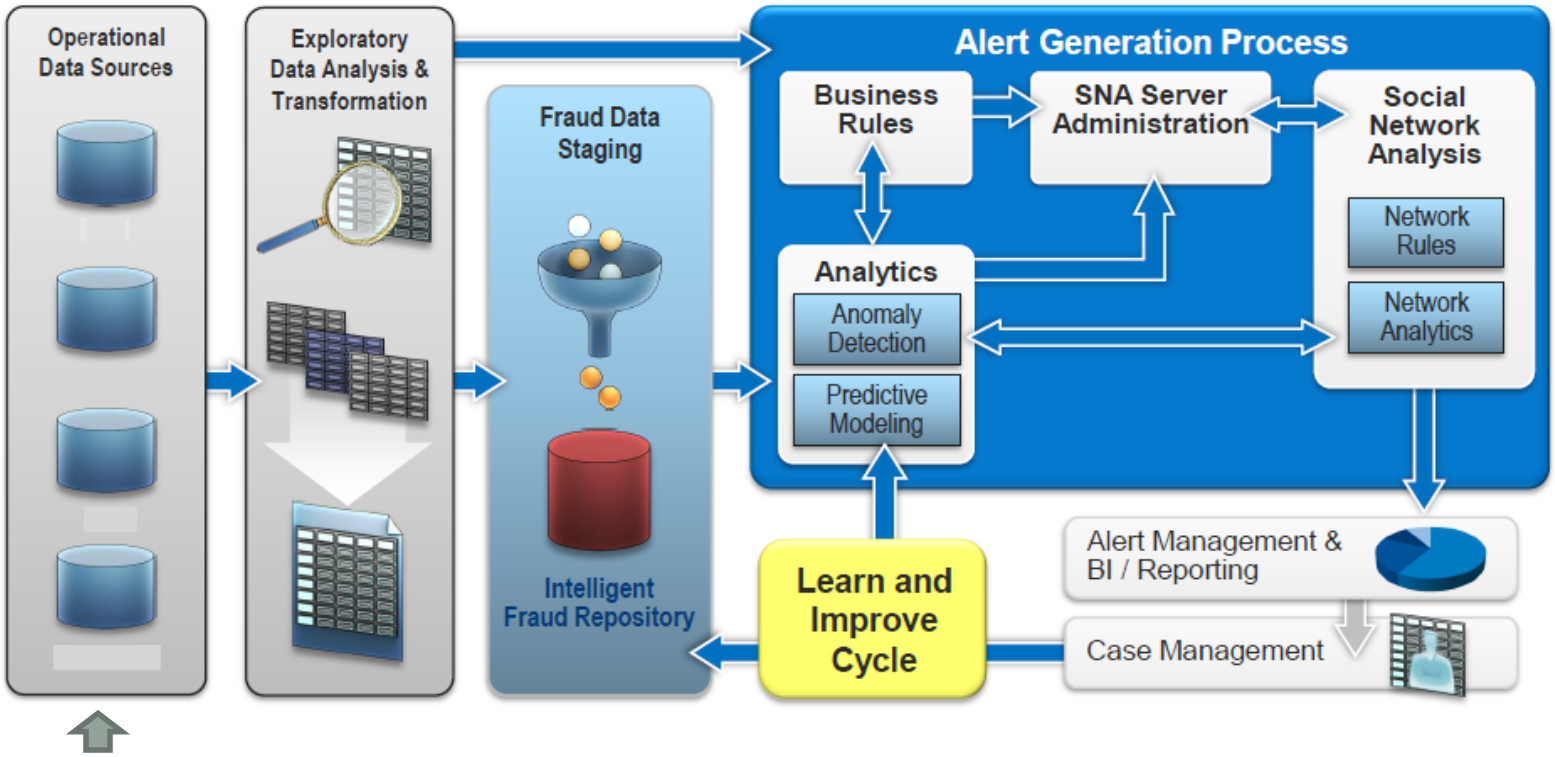
What technology can do to you?

- Here is a video… from Palantir Technologies
- Palantir has specialized in Forensic Technologies

- What typical forensic tools like SAS can do?
  - One big company on predictive real time monitoring as transaction happen! List of their products!
  - SAS – Anti Money laundering solution
  - SAS – Customer Due Diligence
  - SAS – Fraud Management
  - SAS – Fraud Network Analysis
  - SAS – Enterprise Case Management

Forensic Framework for Tools

Process Flow



Various Data Analytic tools

- Old Generation tool
  - ACL
  - Idea
  - Arbutus (almost like ACL)
  - Even Microsoft Excel or MS SQL
- New Generation Tools
  - SAS
  - R Project
  - Python based solutions
  - Oracle Data Analytics
  - Verafin (US company specializing only in banking fraud and AML)
  - Other solutions incl text mining like Semantria, Synapsify, Luminoso etc.

Fraud Management system

- SAS – Fraud Management
  - Banks have implemented this successfully… See this video
  - Behavior Detection Technology BDT & Pattern Detection
  - Proactive Case management
  - Preventive Vigilance

Behaviour Detection Technology

- Components of BDT are
  - Scenarios
  - Thresholds
  - Alerts
  - Look back period and its frequencies

- The architecture of BDT is that it must have a
  - Source system (CBS, delivery channels etc)
  - BDT Platform – This is normally SAS or Mantas or Searchspace etc
  - Alert Analysis Tools – These are generated using workflow / reporting tools.

Pattern Detection

- Transaction monitoring systems,
  - Focus on identification of patterns of transactions leading to Suspicious Activity .
  - Identification of suspicious (as opposed to normal) transactions is part of the KYC requirements.
- Currency Transaction Reporting (CTR) systems,
  - which deal with large cash transaction reporting requirements (Rs 100,000 and over)
- Customer identity management systems
  - which check various negative lists and represent an initial and ongoing part of Know your customer (KYC) requirements.
  - Electronic verification can also check against other databases to provide positive confirmation of ID such as in India Aadhaar or in CIBIL

  (the "share" database used by banks and credit agencies; telephone lists; electricity supplier lists; post office delivery database)

Illustrations 1 (operational)

- **Skimming**
  - Short time deposit and withdrawal on the same account.
  - Deposit made and OD taken immediately
  - Find indicators of kiting checks.
  - Highlight duplication of credit card transactions and skimming.
- **Larceny**
  - Identify customer account takeover.
  - Identify co-opted customer account information.
  - Locate number of loans by customer or bank employee without repayments.
  - Find loan amounts greater than the value of specified item or collateral.
  - Highlight sudden activity in dormant customer accounts – identify who is processing transactions against these accounts.
  - Isolate mortgage fraud schemes – identify “straw buyer” scheme indicators.
- **Financial Statement Fraud**
  - Monitor dormant and suspense General Ledger accounts.
  - Identify Journal Entries at suspicious times.

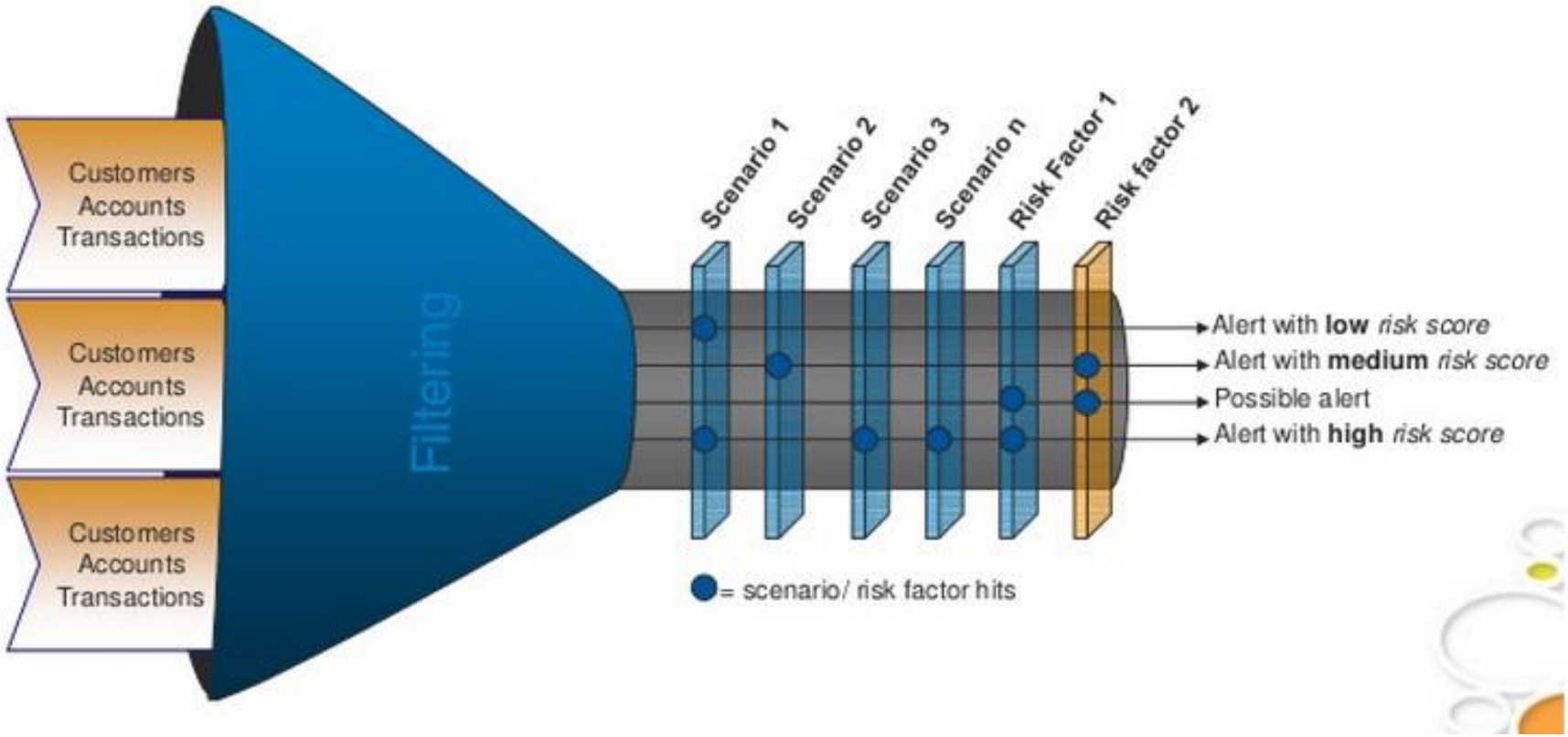
Illustration 2 (Operational)

- Accounts showing activities similar to multi level marketing (MLM) or Ponzi like schemes.
- Large number of cheques getting deposited in inoperative accounts
- Transactions of value just under the regulatory reporting threshold & spilt across accounts to avoid reporting & levy of charges
- Splitting of inward foreign remittances to collect funds in cash in an apparent attempt to avoid fund trail
- Multiple Small amounts debited from customer accounts in the guise of charges, fees etc. and credited to employee account
- Sudden activity in Dormant accounts with large balance.
- Pyramid like transactions (Small value transaction followed by increasingly large value transactions)

Illustration 3 (Technology)

- Same user login from different terminals within short span.
- Requested change in mobile number and surge of transactions
- Requested change in address followed by new PIN request
- Request for a new card and large value / large number of transactions.
- Large number of transaction from same POS/ ATM
- Address change / mobile number change through IVR/Call center and cheque book/ ATM card request subsequently
- Specific/Set of users doing more than certain type and number of exceptions like debit without cheque / User transaction limit exceeded etc.
- Multiple small value remittance to dormant/inactive account and siphoning funds through Swift /RTGS/NEFT

Scenarios and Risk Factors based



Customer Account Transactions are filtered based on business rules that one define keeping mind Scenarios and possible risks and categorize the same as low risk, medium risk and high risk and make response accordingly

What one should look at in a forensic tool?

- **Real-time transaction scoring**
  - Instead of detecting upon happening, it should trigger real-time alerts and prevent something happening
- **Sub-second response time**
  - In credit card authorizations, if normal spend of a customer is say Rs. 10000 per month but suddenly it is to full credit value, decision should be in sub-second speed.
  - HSBC has implemented this solution to trigger feedback and reduce credit card fraud. Predictive models are used by SAS.
- **Powerful advanced analytics**
  - Scenarios and risk factors based alerts
- **Integration with authorization systems**
  - Check for authorizations for exceptions and look for closer to threshold
- **Extensive rule writing and reporting capabilities**
  - Like being done in Delinquency video that we just saw!
- **Flexible alert and case management**
  - Alerts and cases are handled using Emails / SMS / dashboard

FUTURE OF FORENSICS

Proactive Compliance

What will be the future of Forensics in Finance sector?

- The future systems will even look at intent and prevent frauds before they happen!
- **Digital reasoning** is one such software company
- They apply advanced software they use for US Defense , CIA etc to detect terrorist activity to prevent financial frauds!
- This is called ‘proactive compliance’

Why is proactive compliance needed?

- Current machine based fraud detection systems use algorithms to scan trading logs and other structured data to look for suspicious patterns
- But this is an issue as:
  - 70% plus data is unstructured
    - and more importantly
  - It is a slow process- by the time analysts detect potential evidence, the horse has bolted out the door

How is ‘Proactive compliance’ done?

- Synthesys smart software maintains constant vigil over
  - Every small email
  - Instant message
  - Media report
  - Memo etc
- To pinpoint **intentions** to engage in prohibited or illegal activity before they develop into **infractions**
- The crux is **moving from evidence to intention**

How is proactive compliance done?

- Synthesys is the Digital Reasoning's system which
  - Weighs each piece of correspondence against the next to determine probable context
  - It matches recent news headlines with data
  - Takes note of personal relationships and flags abnormalities
    - For instance if some employee suddenly starts emailing some other employee in another part of organisation with alarming frequency
  - System refines its results based on previous successes to better look for tell tale signs of collusion, unreasonable trades or information leaks from within.
  - Policy analytics done along with data analytics
  - In case of AML Analyse narratives within Suspicious activity reports (SARs) and publicly available information for hidden relationships , concealed networks and previously unknown behaviors.

Forensic Audit - Now

- Mostly outsourced by banks
- Focus on detective after initial indicators
- Most times forensic study happens post happening of a fraud
- No population level checks being done
  - Some CMM that is being deployed by banks are more from revenue perspective than Fraud detection perspective
  - Fraud detection is only incidental and focus missing
- There is no focus on preventive forensics using technology
- BIG Data analytics is yet to catch up in banking to focus on forensics

Forensic Audit – In Future

- Banks to implement the systems for Predictive, Preventive and Control of Frauds based on their own experience and knowledge base and risk plan
- Auditors trained in these systems to audit the effectiveness of efficiency of the implementation and its impact on the CAR
- Auditors will develop their own tools once such systems in Banks are standardized and uniformly implemented.
- Audit Reports will be objective , case/data based and uniform for the Central Bank to review and initiate the regulatory and review control measures.