Data Privacy Considerations

By Furaha Marwa

September 23, 2021

Preamble

Data privacy or information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around:

1).Whether or how data is shared with third parties.

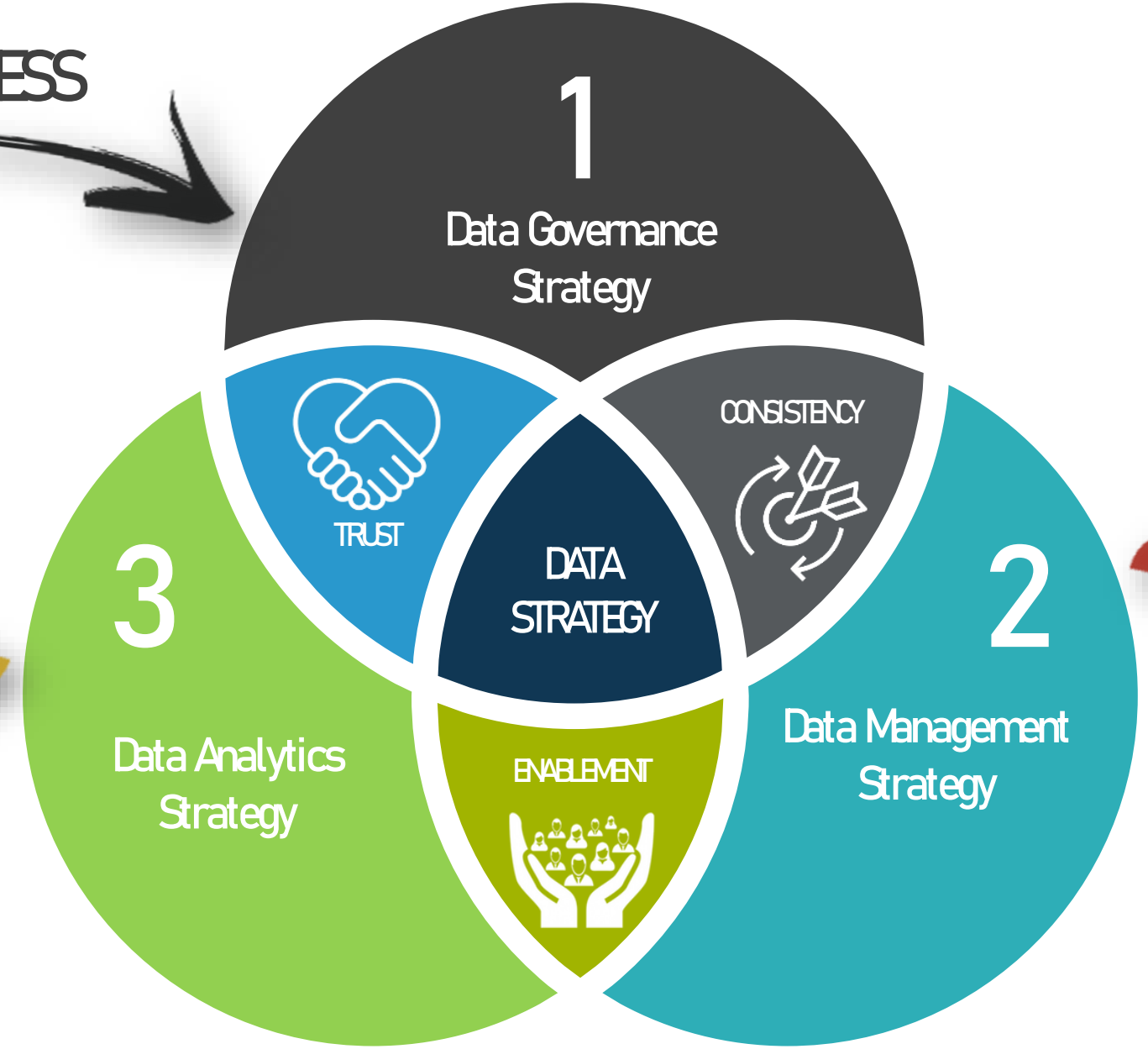
2).How data is legally collected or stored.

3).Regulatory restrictions such as the Data Protection Act, GDPR

Pillars of a Data Strategy

PEOPLE & PROCESS

defines the skills and organization to ensure effective data management and consistent use of data across the entire organization.



DATA & TECHNOLOGY

refers to the impact of data analytics on the business with regard to financials, business processes, customers, and organizational growth

DATA & TECHNOLOGY

Typical data management capabilities refer to, for example, data processing, data provision, data modelling, and data access.

The 6 Most Challenging Data Privacy Issues

- Embedding data privacy.
- Proliferating devices.
- Increasing maintenance costs.
- Access control is difficult in many industries.
- Getting visibility into all your data.
- A long list of regulations and documentation

Develop a Data Governance Vision

To ensure that we hold data that it is **actionable, integrated** and **fully accessible** across the Company to help meet corporate objectives.

Data Protection Act, 2019

Overview of the Data Protection Act

- 2019 –The Data Protection Act ,2019 Enacted
- 2020–Office of the Data Protection Commissioner Established

The Act provides;

- Framework for the right to privacy as it applies to "personal data".
- Practices, safeguards, rules, transparency and responsibility
- Safe collection, processing and storage of personal data
  - The Act shifts some control from institutions to " data subject".

Significant Developments in Kenya's Data Protection Regulatory Landscape

- **Elevated importance of privacy for individuals**

– Emphasis on responsible data practices; non-compliance attract hefty fines/penalties

- **Strengthening Individual Control**

- Enabling individuals to have better control over their personal data. Individuals now have a legal backing and avenues to exercise their data privacy rights

- **Timely response to data breaches**

Notifying the Office of the Data Protection Commissioner as well as any affected individuals within 72 hours

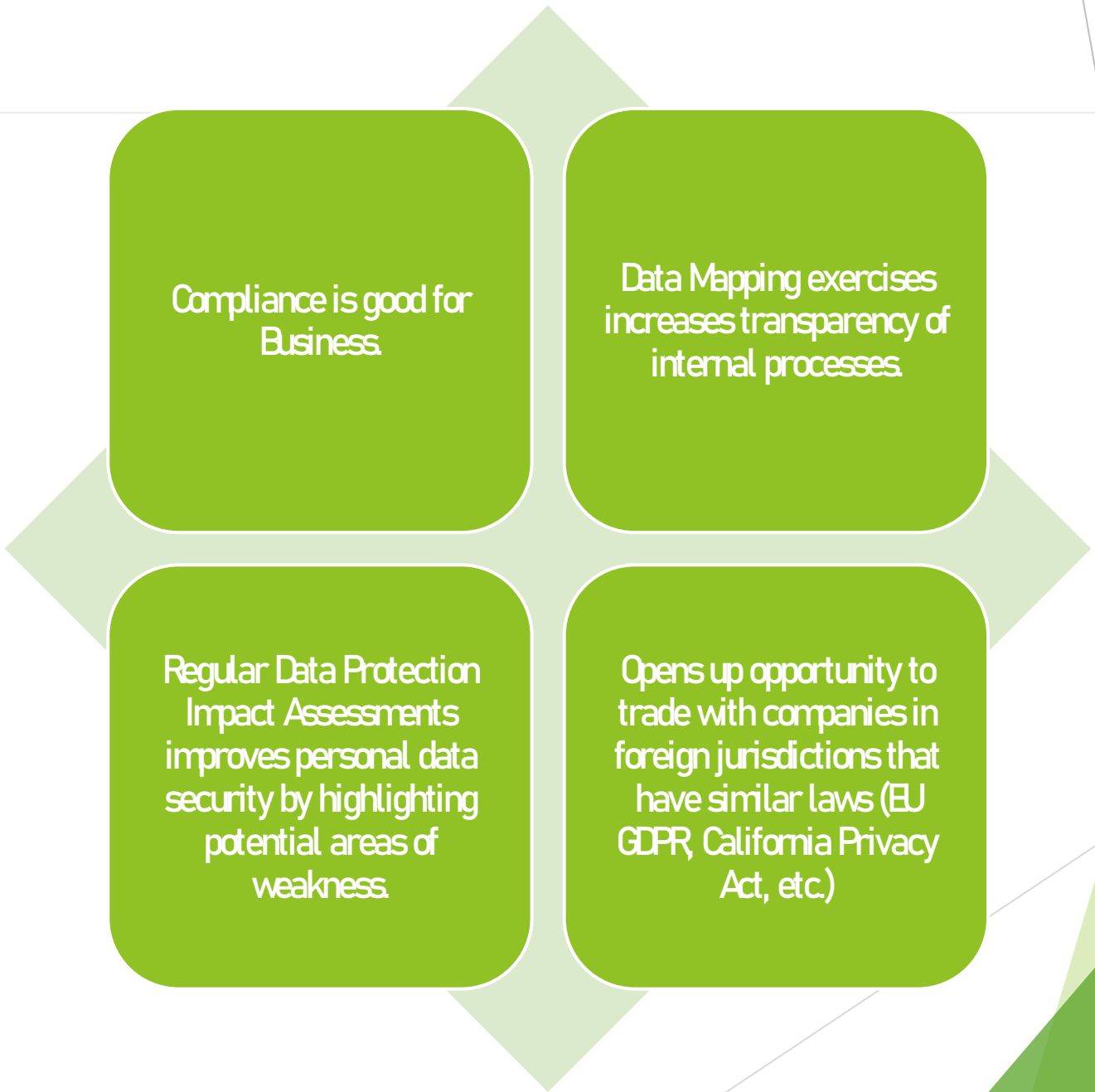
- **Harmonization & applicability to all organizations**

Privacy rules will apply in the same way, and in a clearer way, for all organizations

- **Increased territorial scope**

The Act applies to all processing the personal data of data subjects residing in Kenya, regardless of organizations' location.

Why Privacy & Data Protection Matters – It is Good for Business?



Why Privacy Matters

Lack of compliance is punitive.

Office of the Data Commissioner is mandated to effect sanctions, penalties on violators.

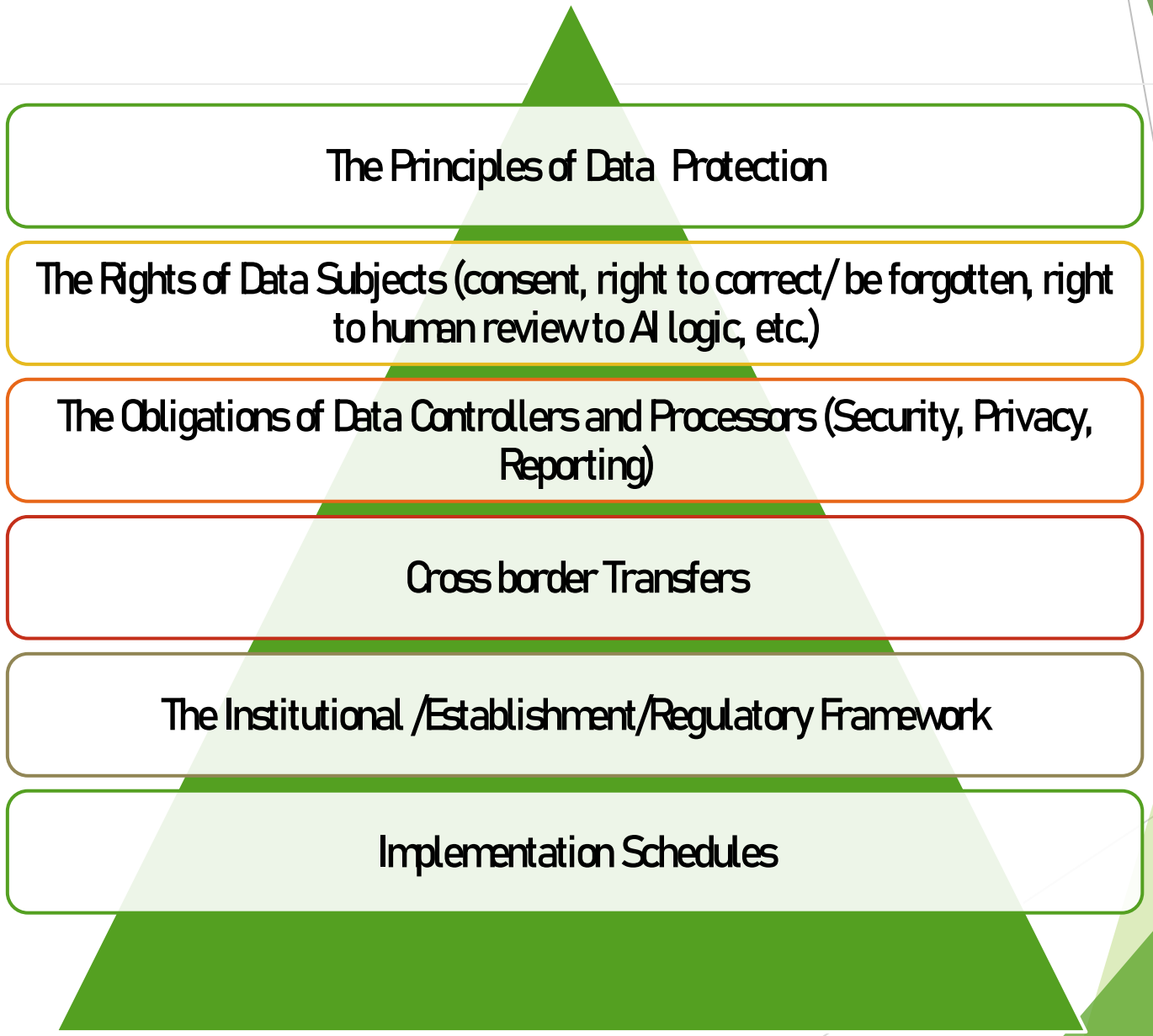
Data Subjects have rights to petition the Data Commissioner over violations, data breaches and seek compensation.

Non-compliant enterprises face costly compliance & reputational risks.

General Penalties (Up to Ksh 3M, 2yrs Imprisonment or both for individual offenders).

Administrative Fines (Ksh 5M, 1% Annual Turnover or Both for corporate offenders).

Key Domains of the Act



The Key Data Protection Principles

a) Fairness and lawfulness (e.g. Consent, Contract, Vital Public Interest)

b) Restriction to a specific purpose

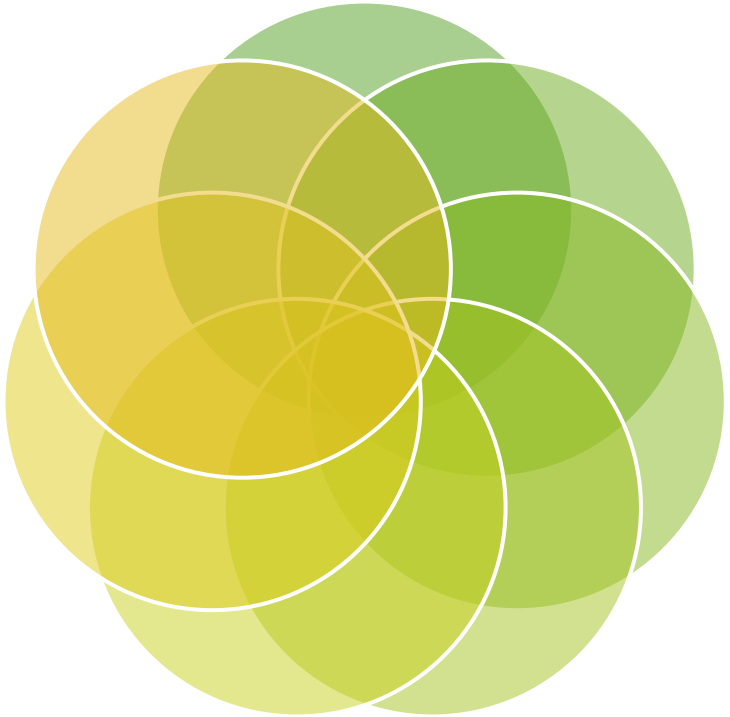
c) Transparency

d) Data minimization

e) Storage Limitation

f) Factual accuracy; up-to-date data

g) Confidentiality and data security



The Data Subject (Citizen) Rights

The Data Controller & Data Processor Obligations (a)

Inform the data subject about the data processing activities and the rights of data subject under the law.

Specify the purposes for which data is to be used.

Should only collect and use personal data in accordance with lawful conditions.

Should keep updated records of processing activities, making them available to the Office of the Data Protection Commissioner and to the data subject on request.

14

The Data Controller/Processor Obligations (b)

Rely on consent as a condition for processing personal data only where: the data controller first obtained the data subject's specific, informed and freely given consent.

Notify the regulator and data subject of any data breach.

Register with the Data Protection Regulator.

Designate a Data Protection Officer to handle all matters of data protection.

15

The Data Controller/Processor Obligations (c)

Conduct Data Protection Impact Assessments.

Develop internal data protection policies and procedures.

Provide privacy notices/notifications to data subject before personal data is collected or used.

16

Key Implications for any institution

Data Privacy & Protection By Design

- Create inventory of Data Processes & their Life Cycle
- Evaluate existing data processing system to establish the extent (or not) that they meet the Key Principles (Consent, Purpose, Data Minimization etc.)
- Undertake Data Protection Impact Assessments

Take note of Breach Notifications to ODC (within 72hrs)

17

Implications for Accountants/Finance Professionals

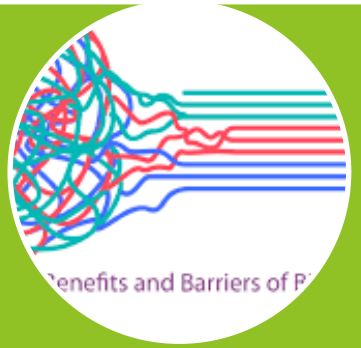
Do you have adequate insurance cover : to cover cyber risks, notification processes, business interruption, Public Relations, etc.

ORACLE

ENTERPRISE
SOURCE PLANNI
CLOUD

For cloud based solutions have you complied with e.g. where you have data sitting in Oracle, SAS or other ERP systems on the cloud?

Contracts going forward: Data Sharing Agreements, Consent before sending data to third parties, clauses to indicate data may be shared with regulators, investigators, auditors,



Have you conducted your data mapping exercises? Do you know where all you data sits and how they are stored?

The use of technology to detect fraud

The key to catching fraudulent actions before real damage is done is having systems in place to flush out anomalies and report suspicious activities early or in real-time.

This means being equipped with tools like

- 1)- Automatic monitoring.
- 2)- Machine Learning and Artificial intelligence.
- 3)- Anomaly detection protocols.

How is this done?

- Data mining and statistical analysis can be helpful in detecting fraud.

- By using sophisticated data mining tools, companies can search millions of transactions to spot patterns and detect fraudulent transactions.

These tools include:-

- decision trees, cluster analysis, association rules, and can generate predictive machine learning models to predict fraud.

Why is Machine Learning and AI Algorithms better?

- Traditionally, organizations have relied on business rules to detect fraud most of which was conducted periodically these are if-then logic rules.

  e.g. if account balance=0 and period >180 Days then status=deactive

- Machine Learning techniques leverage on these rules to build outlier analysis and anomaly detection system
- ML and AI augments these with techniques that introduce pattern recognition, behavioral analysis and symptomatic aspects of accounts, sim cards et cetera

What does ML and AI require?

ML essentially relies on :

- Clean verifiable quality data – Quality data is foundational to building anti-fraud ML systems.
- Multiplicity – There's no single ML Algorithm or model that best works for fraud detection. Success comes from innovations with a mix and match / hybrid approaches.
- Integration – an obvious must-have, but it remains a common roadblock to success in many organizations. Integration is key to the success of ML algorithms.

What does ML and AI require?

- White-boxing: ML methods and models are generally black boxes that need to be explained to decision makers detailing how the model works and what it does.

- Ongoing monitoring: Ongoing monitoring of ML fraud detection systems is imperative for success. A good monitoring program should register and track the ongoing efficacy of all models.

What does ML and AI require?

- Experimentation: Successful ML programs have an element of ongoing experimentation where data scientists and industry players can freely experiment various methods to combat fraud.

Examples

- Predictive machine learning algorithms that predicts whether for example a certain claim is fraudulent. The analysts can then have a closer investigation for the cases that have been marked by data mining software as outliers.

Examples

- Detects the fraud activity and minimizes the risks of the intrusion into a payment system For instance, machine learning can analyze the accidental false positives in fraud detection, thus preventing loss.

- Respond to the unusual aspects of payments. For example, ask for double authentication to confirm and complete a sale transaction in the area of e-commerce organizations.

Bringing it all together

- Fraud detection is a challenging problem. While fraudulent transactions represent a very small fraction of activity within an organization, a small percentage of activity can quickly turn into big financial losses.

Thus, the right tools and systems should be in place. Advances in ML have enabled systems to learn, adapt, and uncover emerging patterns for preventing fraud.

THANK YOU

Furaha Marwa
0701002211
furaha.marwa@analytica-ai.com