dataBelt counter-fraud **use cases**

Data Forensics, Fraud Detection and E-Discovery

1) Data deep search/e-discovery

Identify any and all data sources matching to a text, voice or image, or any associated meta data such as – documents, emails, text strings, images, voice files:

Law enforcement or litigation. Need to:

- Find - in any location - mails, files, text, images, voice recordings, targeted website content for police, legal case or assignment
- Securely share discovered information through secure portal or via secure link to agencies, legal counsels etc
- Discover and redact data sources for legal purposes whilst maintaining an original and full copy
- Undertake a regulatory/compliance review – eg data protection, finance, pension, H&S

Fraud Detection/Counter Fraud. Need to:

- Investigate possible ID theft (eg streaming form source and comparing personal documents, eg passports)
- Check for multiple fraudulent applications from same person, eg benefit or insurance fraud
- Undertake legislative or regulatory review, detailing anomalies pointing out possible fraudulent scenarios
- Investigate supply chain and invoice corruption
- Detect and prevent fraudulent payments by matching name to invoice to PO to bank account
- Detect key words spoken or written that may imply insider or rogue trading, or mis-selling of products
- Investigate crypto currency fraud
- Alert if new payments are set up/unauthorised/not matching defined criteria/not in line with agreed procedures
- Alert when anomalies or unusual patterns occur
- Support fragmented agency investigations and bring financial compliance teams together with fraud, bribery and corruption teams
- Investigate predator lending using data sources to prosecute illegal methods
- Stop improper payments before they happen
- Understand the risk of fraud – who has access to what data, identify need for segregated duties

Data Comparisons and Big Data. Need to:

- Locate and compare datasets for operational purposes:
  - → Supply chain process
  - → Big data analysis

t: +44 (0) 8448 040 653
e: info@aimltd.uk
w: aimltd.uk

Migration. Need to:

- Take on new business or staff (eg through TUPE) and ensure that data migrated is accurate, clean, compliant before import
- Check for, investigate and eliminate rogue data eg phantom employees, suppliers
- Merge multiple datasets & ensure accuracy & compliance – M&A etc

Specific data/information explorations to assist with operational efficiencies, risks, liabilities. Need to:

- Understand content, location and renewal dates of security certificates
- Identify file attachments held on an email system or on a specific drive that need to be extracted and relocated to another location to de-risk document management (Report provided for IT to relocate files, or use data***Belt***'s data***Trove***
- Identify security breaches or anomalous behaviours through: (also see cyber security):
  → Suspicious file movement through data snapshot
  → Incorrect location/jurisdiction of data/files
- Assess data/file classifications - eg business importance, risk, sensitivity, value - to aid with optimal storage solutions and costs
- Pull together an infonomics strategy

Manage data/file/document/records structures

- To ensure they are inviolate and authoritative
- To reduce the risk of financial crime
- To comply with ISO 15489

2) Know/verify your customer

Verify ID (linked to ID theft), check bona fides, criminal charges, age, address etc to ensure the legitimacy of an individual to counter ID fraud.

3) Anti-money laundering

Check for individuals against agency databases – any record or conviction of past money laundering to ensure legitimacy of a financial transaction.

4) People Trace

Find the past location of a person, check ID & bonafides, eg to reunite the correct person with lost pensions.

5) Create reports and counter-fraud dashboards for operatives.