Data Driven Compliance: the use of Advanced Analytics in tackling Fraud & Error

Evert Voorn | Thought leader, Tax & Welfare, Capgemini

Public Sector Forum - SAS Institute Belgium
September 30th, 2016 | Brussels (B)
• Why should Tax & Welfare Agencies move to data driven compliance?
• The impact of technology on Fraud & Error
• How can Tax & Welfare Agencies respond?
• The Capgemini response
Trends in Public Sector Agencies
Tax & Welfare
Public administrations are being re-invented

---

**Growing use of digital**
- Growing use of internet to research and buy private sector products and services – fuelling 24/7 and e/mobile app service expectations
- Explosion in the use of social media – ability to build customer insight but reputational risks

**Financial austerity in the West**
- Stagnating or declining real incomes in the West; fiscal deficits and levels of debt
- Political pressure to address tax non-compliance and welfare fraud

**Globalisation**
- Tax competition between states - large business tax domiciles; inward investment; key skills
- Rapid growth of emerging economies and middle class – demand for welfare state

**Technological developments**
- Big data - new data sources e.g. Social media, smart grid; processing power e.g. Hadoop;
- High performance analytics e.g. SNA, voiceprints – shorter analytical timescales
- Internet transparency

**Industrialisation of fraud**
- Increasing sophistication of banks and insurance companies are driving criminals to attack tax & welfare authorities; testing defences; insider fraud

**Digital by default**
- Push to online applications/change of circumstances and renewals; use of mobile apps / text; voluntary sector support for “needs help” segment

**Improve customer experience**
- Make it simpler for customers so that they comply with the need to inform of change of circumstances and make fewer genuine errors. Design out contact; simplify online forms & guidance and processes

**Data analytics to better target risk**
- Welfare administrations are leveraging new data sources and more sophisticated modelling tools and data mining to improve targeting of high risk cases, detection of fraud and retrieval of debt
- Segmented approach to fraud investigations; graduated range of interventions; moving upstream (prevention)

**Re-inventing welfare administration**
- Process standardisation across benefits; re-platforming; shared services, performance KPIs to drive productivity
- Outsourcing /JVs of selected functions e.g. IT, debt recovery, analytics; new commercial models
Digital’ will fundamentally change the government administration model by 2020...delivering a step change in outcomes.

Data and analytics are at the heart of the digital government administration, informing the ability to deliver a differentiated customer experience, dependant on compliance risk.
Fraud
Phenomenology
Governments agree that there is a problem

Five Arrested After Attempted $500k Tax Fraud
Arrests follow probe into scheme that saw 700 UK citizens' identities stolen

On August 27, 2013 by Thomas Browster

Italian and UK police have confirmed the arrest of five individuals suspected of carrying out a “cyber attack” on HM Revenue & Customs as part of an attempted £500,000 tax fraud.

Bayern Munich boss Uli Hoeness admits tax fraud

Bayern Munich boss Uli Hoeness admits to having evaded taxes for years.

ID theft gang jailed for £2m tax fraud

ID theft gang jailed for £2m tax fraud

© 21 Aug 2013

Four members of a Southampton-based organised crime gang, who stole more than 3,000 identities in an attempt to defraud £2m of income tax, have been jailed following an investigation by HMRC.

Germany to probe welfare fraud by immigrants

Germany to probe welfare fraud by immigrants

Agence France-Presse | January 8, 2014 6:18pm

Public servants are investigated over €1.3m social welfare fraud

Independent.ie | Irish News

Public servants are investigated over €1.3m social welfare fraud
The fraud landscape spreads from simple opportunistic non-compliance to organized crime.

- **Taxpayer Segment**
  - Opportunistic
    - Casual Avoiders
  - Purposeful Criminals
  - Organised Crime

- **Level of Sophistication of Fraud**
  - Opportunistic
    - High Volume/Low Value
  - Game Playing
  - Systemic
    - Low Volume/High Value
In response, fraud and error prevention measures with different sophistication must be applied (and at different point of the business process).

Source: SAS Institute
Trends in Compliance Strategies
The deployment of Risking is evolving to data driven Compliance.
So why would this affect my Compliance approach?

- growing demand for and expectations of public services
- growing complexity
- reducing costly investigations
- Industrialization of Fraud
- internal Fraud
- growing use of digital
- growing fiscal deficits
- new & more data
- shorter reaction times
- identity theft
- new modelling tools & techniques
The world is changing and this drives the need for a more engaged, holistic and efficient model of risk management

<table>
<thead>
<tr>
<th>“Our relationship with our customers is evolving”</th>
<th>“There is greater pressure to operate more efficiently”</th>
<th>“New technology is changing how we do things”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer expectations are driven by assumption that organisations should leverage insight they hold about them</td>
<td>Less appetite for risky ‘big-bang’ programmes</td>
<td>Accessibility: more accessible to organisations and their customers</td>
</tr>
<tr>
<td>Diversity in population creates a specific type of demand on service delivery models</td>
<td>New delivery models with shared accountability</td>
<td>Ease of use: enabling seamless flow from back-end to front-end</td>
</tr>
<tr>
<td>Greater migration and mobility</td>
<td>Joined up services</td>
<td>Automation &amp; volume: systems becoming increasingly automated and able to process higher volumes of data</td>
</tr>
<tr>
<td>“Individuals and organisations are more globalised”</td>
<td>“There is a shift towards working more openly”</td>
<td>Agile: new delivery models</td>
</tr>
<tr>
<td>Collaboration and/or competition across borders</td>
<td>Customer expectation of transparency in every interaction</td>
<td></td>
</tr>
<tr>
<td>Complex international financial arrangements</td>
<td>Privacy concerns</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data is being shared more actively</td>
<td>New types of technology enabled fraud (phishing / zapping)</td>
</tr>
<tr>
<td></td>
<td>Shift towards open source and open data</td>
<td>Increased speed of fraudsters</td>
</tr>
<tr>
<td></td>
<td>Non-repudiation</td>
<td>Security</td>
</tr>
<tr>
<td>“We need to respond to new threats”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased frequency of cyber attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New types of technology enabled fraud (phishing / zapping)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased speed of fraudsters</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Management was traditionally seen as a specialised capability, focusing on threats which were already transacted and driving corrective actions.

Capabilities supporting this model were usually siloed across the organisation, less synchronised and focusing on individual transactions/products with lack of holistic view of customer’s risk.
To enable that, the transaction-based industries will have to build deeper insight into their customers and leverage it more pro-actively.

At the core of the global trends is a need to:

- **Build more insight**: create a more holistic view of customers, their circumstances and behaviours

- **Leverage this insight more proactively**: Change from reactive (downstream) driven organisation to one that actively drives interaction with customer and prevents risk

This translates differently across industries:

- **Tax**
  - Treat customer holistically across tax types
  - Lower the cost of compliance
  - Counter through complexity of globalised financial relationships

- **Welfare, Health & Social Care**
  - Address demographic changes through more diverse customer service
  - Leverage customer insight to prevent overpayments and sustainably reduce Fraud & Error levels

- **Grants & Funding**
  - Improve insight into risks in respective stages of the funding value chain
  - Prevent inefficiencies in spending

- **Banking**
  - Improve KYC in the growing complexity of financial relationships (often cross-border)
  - Manage Digital Transformation and all channel experience

- **Insurance**
  - Become more engaged with customers throughout the lifecycle and update products based on their circumstances
  - Increase claim efficiency and enable X-channel straight through processing
But you need to tailor it to the type of non compliance at the right phase in your business processes.

Anti-fraud methods need to be highly integrated into the normal business process. The processes focus on whether to accept and process the transaction using IT to assess the transaction and identify the risk of processing it.

The risk level is determined by a combination of rules and indicators inherent within the transaction data, or against reference or historical data, including:
- Transaction characteristics—channel, submission, size, type, etc
- Credibility tests—assessing the transaction against previous history
- Reference data—assessing variation from known data
- Fraud patterns—comparing the transaction to known fraud (or error) patterns
- Anomalies—identifying transactions that suggest fraud or error patterns of behaviour and that might indicate fraud.
- Use of Social Network Analysis (SNA) to show links between data items

Typical techniques are through the use of entity analytics to produce a complete view of a taxpayer entity (business or individual) to see the correlation between different activities and identify significant outliers that may indicate fraud or non-compliance.

Other techniques that can be usefully employed are Social Network Analysis that identifies links at the data item level, often showing links that are not explicitly declared by the taxable entity.
The Non compliance Maturity Journey of modern Public Organisations

Non Compliance Maturity

Time

Your Current position (?)

Advanced Analytics

Use statistics to predict future non-compliance

Expert Rules

Apply exception based rules, including tip-offs, to identify suspicious behaviour

In-Process Controls

Implement in-process controls to stop and catch non-compliance

Specialist Investigators

Build special Investigation Unit focused on non-compliance
How will Technology impact the fight against Fraud & Error?
We are all aware of the rise of ‘Big Data’...

- Many PBs of data every day
- 25+ TBs of log data every day
- 12+ TBs of tweet data every day
- 30 billion RFID tags today (1.3bn in 2005)
- 4.6 billion camera phones worldwide
- 100s of millions of GPS enabled devices sold annually
- 2+ billion people on the Web at end 2012
- 76 million smart meters in 2009...200m by 2014

80% Of world’s data is unstructured
...but it is how you analyse that data that will be key to future success

Business Analytics is the use of advanced analytical techniques to **find trends** and **predict future outcomes** which are used to **optimize business processes, customer interaction** and **manage risk and fraud**.

**Business** – it is the use of analytics to directly target a business issue or process and as such is sold to the Business. Examples are customer retention, increasing wallet share, fraud reduction...

**Analytics** – it makes extensive use of data, statistical and quantitative analysis, explanatory & predictive modeling, and fact-based management to drive decision making.

Governments will have to become data-driven, analytics-enabled organisations
Moving faster to an analytics enabled world means a shift in our Big Data thinking.

- Big data is driven by business use cases
- Each area can get their own insights
- The Business Data Lake provides a place to land the big data
- Each business area can have their own analytics on the same data

Insights can then be shared across the business.
So we will need data lakes to support this new world of analytics

- Store everything
- Treat global as a local view
- Govern only the common
- Encourage local

It's all about insight at the point of action
But Governments will also have to operate in a digital world with increased risks for fraud and error.

Nation States – Hacktavists – Organised Criminals

Pre-Authentication Threats
- DDOS Attacks
- Phishing Attacks
- Parameter Injection
- Vulnerability Probing
- Risking
- Intelligence Gathering

Post-Authentication Threats
- Man in the Browser
- New Account Registration Fraud
- Account Takeover
- Fraudulent Reclaims
- Login
- Password Guessing

Disruption and/or Intelligence Gathering

Transaction and Logout

News > UK > Crime

Cybercrime boss offers a Ferrari for hacker who dreams up the biggest scam

Major emerging Trends in Fraud Management

- **Centralization of Fraud Management Operations**: To effectively fight fraud, forward-looking financial firms constantly update fraud management systems with new rules, statistical models and acquired knowledge. This process becomes easier and more efficient with centralized systems.

- **Usage of More Real Time External Data**: Several financial services institutions are no longer content with just using regular transactional data to fight fraud and are also looking at external information obtained from third party vendors and intelligence from social networking sites to improve their capabilities in fraud detection.

- **Rise of Cyber Crime increased by the adoption of mobile devices and the use of external data**: Consumers want simple, easy-to-use banking services, but do not accept that they are vulnerable to fraudulent activities. Organizations which are able secure their transactions by moving to the next generation of authentication, such as biometric authentication enabled through mobile technology, can create competitive advantage by meeting consumers’ expectations for products that are both simple and secure.

- **Use of advanced analytics methodologies on a single fraud management platform combining...**: Incorporation of a Hybrid approach to analytics

- **Out of pattern analysis**: Comparing customer activity with peer group behavior, and also with the customer’s own past behavior to identify outlying transactions.

- **Linkage analysis**: Identifying other entities associated with known types of fraud, as well as practices used by fraud-linked entities – sometimes using analysis of social networking activity – and developing strategies to counter these practices.

- **Model development**: Creating fraud-scoring tools and detailed statistical analytics to provide quantitative insight into possible fraud activity.

- **Rule development**: Creating and applying rules for basic business activities to spot unusual trends, as well as specialized rules for specific transactions.
Focusing on fraud, current detection systems only hit the tip of the iceberg

Current versus Most Advanced Fraud Detection Systems

- **Review**
  - Retroactive
  - Obvious standard patterns, hot-lists of known schemes
  - Minimal or ad-hoc feedback loop

- **Rules**
  - Models using thresholds
  - Detect linear relationship only

- **Review → Detect**
  - Predictive (early detection)
  - Detect subtle cases
  - Constant feedback loop (learning models)

- **Rules → Advanced models**
  - Capture predictive non-linear behaviors
  - Adapt to constantly evolving fraud patterns

- **Multi-dimensional Big Data fraud systems**
  - Leverage highly fragmented/incomplete data
  - Create multiple linkages (claimant profiles, auto-body shops, physicians, adjusters, crime rings, micro-geo inputs, etc.)
  - Convert categorical and text-based data into predictive signals

- **Decision tools** (from pull to push, intuitive interface flagging cases, real-time interactivity)
Example of Applied Analytics:
Uncovering fraudulent VAT Carousels
With Social Network Analysis
Some explanation of what we did: VAT Carousel Fraud – Basic Pattern...

Process Diagram

1. A sells goods to B for €1m. No VAT as A is in different EU country from B
2. B sells goods to C for €900k plus €180k VAT. B never pays €180k VAT to Belastingdienst and "disappears"
3. E sells goods to A for €950k. No VAT due as A is based in another EU country. C claims refund of VAT of €180k charged by B

Country 1
Country 2

Criminal Attack
Missing Trader
Buffer Traders

Tax Authority
VAT Carousel Fraud – Presented Pattern
VAT Carousel Fraud – A network after investigation
VAT Carousel Fraud – Getting the picture...
Next step: moving from Investigating networks..... To event oriented risk assessment
Lessons leaned

In the effective use of Applied Analytics:
Lessons Learned: building a compliance capability

Think big...

- The use of the enormous amount of available data (both public and private) to increase your compliance capabilities and effectively implement large scale fraud detection and preventing measures implies significant investment in business and technology change, supported by strong governance.

- Organisations typically start by designing a target operating model, enterprise architecture and enterprise data model that sets out how they will achieve improved predictive & downstream compliance outcomes. They supplement this with a gap analysis of current capabilities, a route map and a business case.

...Start small

- Experience from other countries shows that developing a wide compliance is a 4-5 year journey.

- Identify an initial customer segment to design, build and roll out an integrated business-IT cross-value chain solution (policy, process, organisation/governance/capability, data model, technology tools).

- **Prove it, then scale it** – then address a second segment applying the same common capabilities.

... It’s not just about technology

- Successful projects started by bringing together business expertise, data expertise and technology expertise working very closely together in incubation chamber circumstances.

...There is no one size fits all
Our credentials in Tax & Welfare
Capgemini comprehensive compliance solution services are based on an ecosystem of strategic alliances and partners.
Our capabilities

**Domain expertise**
- Partner to 35 Tax & Welfare globally
- Understanding of the Tax business process
- Compliance Framework
- End to End solution
- World’s foremost provider of Business Information Management (BIM) services.

**Delivery capability**
- Strategic global partnership with SAS on Fraud management solutions
- BIM Centre of Excellence in India
- Business & Solution Architects
- Local footprint.

**Proven value**
- Proven success stories in UK, Netherlands and in the Financial Services Sector
- £2.6bn additional tax yield to date for HM Revenue & Customs.

Our Thought leadership
About Capgemini

With more than 130,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2013 global revenues of EUR 10.1 billion.

Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.