Cabinet Office

Department for Digital, Culture, Media & Sport

Thought Paper
June 2019

Tackling fraud in Government with data analytics

Starting the conversation

This document is available in large print, audio and braille on request. Please call +44 (0)207 123 4567 or email enquiries@department.com

Cabinet Office
35 Great Smith Street
London SW1P 3BQ

Publication date: June 2019

Produced by the Centre of Expertise for Counter Fraud, part of the Cabinet Office.

Contents

Kevin Foster MP
Minister for the Constitution

Ministerial Foreword by Kevin Foster

Over the last few years, we have seen the public sector fraud landscape change dramatically. The evolution of digital technologies and data is creating exciting opportunities for individuals, businesses and the rest of society, but it also making the threat of fraud more complex.

This is why the Government is investing in the effective and responsible use of data: to protect our public services from the constant and evolving threat of fraud.

Fraud is an unfortunate reality in any large organisation, and public bodies are no different. Government estimates fraud and error loss at £31-£49 billion each year[1].

Fraud can undermine the Government's ability to address the issues that the British people care about; the NHS, the building of new homes, or supporting our armed forces. This Government is not prepared to accept this, and it is determined to help build a more caring society for everyone and a fairer, safer economy to do business in by fighting fraud.

To fight fraud, you first have to find it. This Government is committed to finding fraud, and the use of data and analytics is one of the ways we can do this in the modern world.

There is already a lot of vital counter fraud work being carried out across Government, both in investigating identified cases of fraud and also in developing new ways to detect and prevent it. However, we know that to uncover the full extent of fraud across the public sector we need to be using twenty-first century solutions.

The public expect the Government to be sharing and analysing data responsibly, but they also expect us to be using all the tools available to protect the public services so many people depend upon. Meeting these two expectations is at the forefront of the Government's approach to using data to fight fraud.

Those working in the public sector are achieving great things - but the public sector does not have all the answers. The private and charity sectors are facing similar challenges and those in academia are increasingly looking at developing the thinking in this area.

This is why your feedback to this paper is an essential next step. We know there is a wealth of expertise and experience out there, and we want to ensure that the wider-counter fraud and data analytics communities have the opportunity to work with Government, and help us shape the role of data in our counter fraud response.

Fraud attacks on the public sector are unacceptable, but this Government is not going to be complacent. We want to proactively find and tackle fraud, and stop the people who commit it. I am asking you to respond to this paper and add your insight to how Government should be using data in the fight against fraud.

Kevin Foster MP
Minister for the Constitution

1 https://civilservice.blog.gov.uk/2018/10/04/5-things-to-know-about-fraud-and-why-were-launching-a-counter-fraud-profession/

Margot James
Minister for Digital and the Creative Industries

Ministerial Foreword by Margot James

Today's digital revolution is being driven by the use of data. Within Government, we recognise the value data plays in delivering better outcomes for citizens. Investing in data not only helps government be more intelligent and informed, but also more capable of making better decisions day-to-day.

Data is a critical part of our national digital infrastructure, which is why, as the government lead for data policy, DCMS is looking to develop the first ever National Data Strategy. We will be working with colleagues across Government and the wider UK economy to develop the strategy. Its overarching aim will be to unlock the power of data across Government and the wider economy; while building public confidence and trust in its use.

A key element of this work is making sure data is used in a safe and ethical way. We have already published our Data Ethics Framework, setting out clear principles for how data should be used in the public sector. We have also established the Centre for Data Ethics and Innovation. The Centre is an advisory body to make sure data and AI delivers the best possible outcomes for society, in support of its innovative and ethical use.

As set out in this paper, opening up data in a way that makes it reusable and easily accessible, while taking into account legal and ethical considerations, can deliver a number of positive benefits for the Government, citizens and the economy.

For instance, a huge programme of work in recent years to promote the open and transparent use of data has culminated in over 44,000 datasets being published on data.gov.uk. This unprecedented level of openness has created many benefits, for example, publishing contract data allowed officials to find millions of pounds of savings through removing duplication.

The work Cabinet Office is contributing around using data and data analytics to combat fraud is another great example of how being more data driven can deliver real benefits. The case studies on the use of data to tackle fraud in this paper will help to build better citizen understanding of government data sharing and bring to life the value and importance of data. Greater transparency of the use of data by the public sector can help illustrate the public good that can be derived from data being more open and more easily accessible. As the paper sets out, it is also important that Government continues to work with the public and private sector to build public confidence in the use of data and address outstanding issues and challenges, such as those associated with data quality, access and analytical capability. This thought paper can play an integral role in achieving these aims.

Margot James
Minister for Digital and the Creative Industries


MEDIA
-SHOW BUSINESS
-NETWORK
-MUSIC
-CINEMA
-BUSINESS/FINANCE
-WORLD NEWS
-INTERNET
-LIVE CHAT
-MEDIA
-PHOTOS
-VIDEOS
-MUSIC
-CULTURE
-ECONOMIC
-FINANCE
-BUSINESS
-MEDIA
-PEOPLE
-CREATIVE
-TUTORIALS
-INVESTMENT
-NETWORKING
-VIDEO
-MUSIC
-FILMS
-SERVICES
-CONTACTS
-MESSAGES
-BUSINESS/
-WORLD NEWS
-PEOPLE
-FORUMS
-MAIL
-SHOP
-BUY
-SALE
STRATEGY
PLAN
INVESTMENT
INCOME
MONEY

Introduction

The aim of this paper is to start a conversation with citizens, academia, industry, and across Government on the use of data and analytics to counter fraud.

To help drive this conversation this paper is divided into three sections:

1 **Using data to counter fraud (p. 10-14)**

An insight into the nature of counter fraud in Government and into the work being done in the Cabinet Office and the Department for Digital, Culture, Media & Sport to advance the use of data and data sharing as part of the Government's counter fraud strategy.

2 **Some key challenges to making even more progress (p. 15-19)**

A summarisation of the key challenges identified by Government, industry, and academia in making more use of data for counter fraud. These are the issues we seeking your input and insights on.

3 **Your voice (p. 20)**

Where we ask for your input on our key challenges; how could Government approach these issues and is there anything else we should be concerned about based on experiences in your own industries?

In the rest of the document you will find the verbatim contributions from the public and private stakeholders – Government departments, academia, and industry – which are the source of the challenges identified in section 2.

1. Using data to counter fraud

The Government estimates that fraud and error costs the public sector £31-£49 billion every year[1]. Sadly, fraud is a reality in any large organisation, but in the public sector it takes money away from vital public services that citizens depend on and damages trust in Government. This is a problem faced by all public bodies and it is one that will only grow as digital channels provide new opportunities for fraudsters to exploit. That is why this Government is committed to fighting fraud and why it has consistently invested in its counter fraud response across the public sector.

In recent years we have changed the way we think about fraud. The Government recognises that economic crime is exceptionally difficult to measure[2], and fraud is no different. People who commit fraud understandably try to hide it and the crime can remain undiscovered or unreported by the victim. This means that to reduce fraud, an individual or an organisation has to first make a deliberate effort to find it.

That is why the Government provides a clear message for all public bodies: to fight fraud, you have to be proactive in looking for and finding it in your organisation.[3] Using data effectively and responsibly is part of the Government's strategy to find more fraud.

1.1 Supporting the use of data analysis from the centre

The Centre of Expertise for Counter Fraud is a central team in the Cabinet Office that leads on continuing to improve the standard of counter-fraud work being done across government. The Centre of Expertise exists to bring together an evidence base for fraud from across departmental boundaries, giving a single picture of the nature and scale of fraud, and enabling all of Government; from central ministries to local authorities, to tackle fraud effectively.

1.1.1 Recognising the power of data

In the twenty-first century our citizens and businesses expect the public bodies that hold and manage their data to do so in a secure and sensible way. They also expect the Government to protect vital public services, and the money that funds them, from fraud using modern, efficient methods.

The private sector is already using data in structured and innovative ways to manage the risk of fraud. The public sector should be no different, and in fact it can also share and learn from partner organisations in the private sector. This is increasingly true as machine learning and Artificial Intelligence (AI) allows us to start generating insights from structured and unstructured data.

The Centre of Expertise has been leading development of the Government's Counter Fraud Function's use of data to fight fraud. Working with public bodies to enable the sharing and cross-analysis of data, it has repeatedly found evidence that demonstrates the vast potential of using data to fight fraud, in the form of recoveries, cost savings and the development and refinement of counter fraud systems.

2 'Economic crime: Anti-money laundering supervisions and sanctions implementation', House of Commons Treasury Committee, 27th report of Session 2017-2019 (HC 20100, p.7)

3 See the Cross-Government Fraud Landscape Annual Review 2018 at: https://www.gov.uk/government/publications/cross-government-fraud-landscape-annual-report-2018

1.1.2 We've been investing in data

Data is being used by counter fraud specialists and data analysts across departments to fight fraud. Their work is absolutely necessary for the cross-government Counter Fraud Function in its agenda of finding and tackling more fraud.

At the centre of this function the Centre of Expertise is investing in providing tools and legislation to support the wider-function, and in building counter fraud capability across government. This investment is delivering the following initiatives:

Providing tools and legislation

- Implementing legislation to provide better access to data and data services, such as the Local Audit and Accountability Act (2014) and the Digital Economy Act (2017). This legislation has provided public bodies with a robust legal gateway to share data with one another in a simplified and responsible way.
- Delivering counter fraud data sharing pilots using a rapid application approach that allows quick testing and evaluation of analytical techniques for tackling particular counter fraud problems across government. These pilots have developed standards and re-usable components that facilitate further cross-government working and data usage.
- Managing the Counter Fraud Data Alliance (CFDA), which has provided a governance structure for sharing data between specific public bodies and private organisations as a pilot, to test the value of such collaborations.
- Managing the National Fraud Initiative (NFI)[4], established in 1996, which created and runs a data matching solution - available to all government departments - to detect and prevent fraud. Since 2016 the NFI has saved the taxpayer over £300 million by finding fraud and error in the public sector.

Building Capability

- Coordinating a new Counter Fraud Data Analyst Community to support the development of counter fraud analytics capability across government. This group actively shares the learnings from their work and distributes knowledge on such effective data sets and analytics techniques for counter fraud, creating a common base for further development of new projects.
- Creating a Data & Analytics Discipline, as part of the Government Counter Fraud Profession (GCFP)[5], to establish common and transparent standards for counter fraud data analytics across the public sector, and beyond.
- Developing and delivering best practice guidance and training on how to pilot the use of data analytics in counter fraud, based on insights from across government and the private sector. This guidance is intended to develop capability in government organisations; facilitating the planning and implementation of more counter fraud data sharing projects without their being dependant on Centre of Expertise support.

4 Find out more about the NFI here: https://www.gov.uk/government/collections/national-fraud-initiative
5 Find out more about the GCFP here: https://www.gov.uk/government/groups/counter-fraud-standards-and-profession

1.1.3 Insight-led data development

The Centre of Expertise and the wider Counter Fraud Function have shown the benefits data analytics can bring to counter fraud. This Government wants to go further, and it wants to work with other sectors and citizens to understand what 'further' looks like.

Knowing how to use data effectively and responsibly is going to be paramount to any organisation that wants to protect itself from fraud in the twenty-first century. Public bodies are no different.

1.2 A cross-government digital and data policy

The Department for Digital, Culture, Media and Sport (DCMS) is responsible for digital and data policy within government. Unifying these policy areas in one place gives DCMS the responsibility of looking across the whole spectrum of the digital economy. It also means policy on the use of data in the wider economy, including data protection, data ethics, and the value of the data economy sits with one strategic lead. DCMS works closely together with departments across Government to realise the benefits of effective data use. This includes working closely with the Cabinet Office on their work using data to combat fraud against the public sector.

Data-driven government: Data is a critical resource for enabling more efficient, effective government and public services that respond to users' needs. The Government collects, holds and uses a large volume of personal and non-personal data in the course of fulfilling its responsibilities. Data enables all kinds of services we use everyday from maps on our smartphones, to social media and payment processes.

Without access to good quality data, AI technologies cannot deliver on their promise of better, more efficient and seamless services. This is why data is so critical to our digital infrastructure and why DCMS will be looking to create a National Data Strategy, to unlock the power of data across government and the wider economy, while building public trust and confidence in its use. In order to take forward the National Data Strategy we will continue to engage with a wide range of stakeholders to look at issues such as public trust in the use of data, data ethics and what the rules of engagement around data should look like.

Open data: The Government is committed to opening up more data in a way that makes it reusable and easily accessible. This is underlined in the fourth Open Government National Action Plan that makes commitments to increase public participation in Government. This can help fight fraud by shining a light upon the full pattern of Government procurement and spending and being explicit about who Government is doing business with.

Data sharing: Data sharing is another integral component of ensuring a more data driven Government and supporting efforts to combat fraud against the public sector. Essentially, delivering public services more effectively and efficiently requires joining together data from multiple public sector bodies. An important aspect is the introduction of information sharing provisions within Part 5 of the Digital Economy Act 2017 (DEA). Public sector access to data has been hindered by a complex legal framework that has grown piecemeal over time. Public authorities have found it increasingly difficult to understand what information they can share. The powers within Part 5 of the DEA are designed to help overcome these legislative barriers. The codes of practice associated with the information sharing provisions set out how the powers must be operated. The data sharing powers arising from the DEA must be exercised in compliance with the Data Protection Act 2018 thereby ensuring data is handled securely, safely and proportionately. There are clear restrictions on who can share

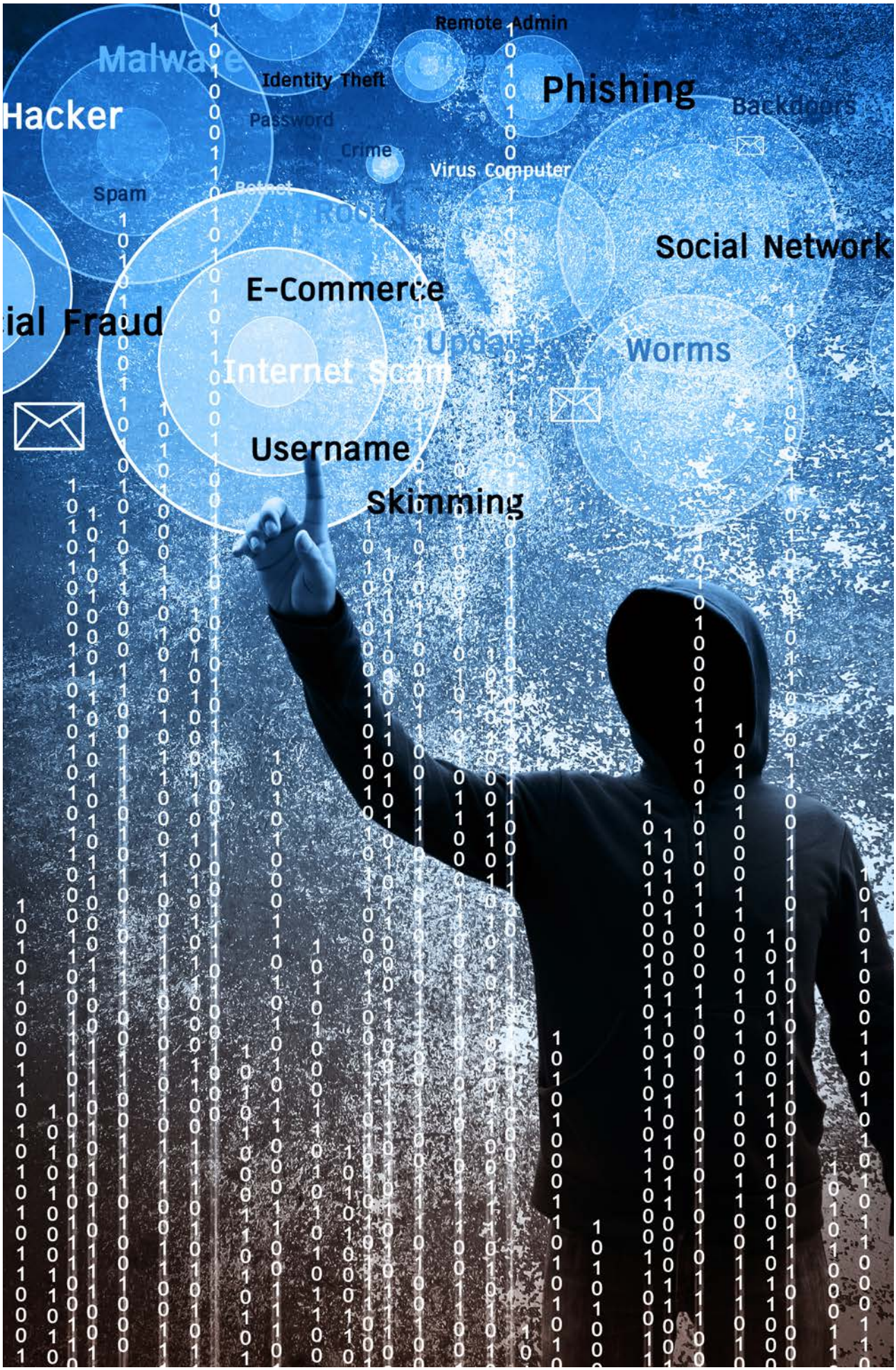
information and for which purposes. Chapter 4 of Part 5 of the DEA enables the sharing of information between specified bodies to better combat fraud against the public sector. As set out in this paper, the use of this legal power to share publicly held information to combat fraud is already yielding positive results.

Furthermore, the Government is committed to exploring data sharing frameworks such as data trusts. The UK Government's Office for AI, along with Innovate UK, partnered with the Open Data Institute (ODI) to successfully complete the first in depth research programme on the role of data trusts. The ODI published its reports from this work on 15 April 2019.

Data ethics: While more open and easier access to data is something that we must aspire to, it is essential that data and Artificial Intelligence is always used safely, securely and in an ethical way. As well as ensuring compliance with data protection legislation when using data, it's also imperative that organisations have regard for the ethical dimension. To support this, the Government has already published our Data Ethics Framework, which sets out principles for using data, in order to encourage ethical data use. We have also established the new Centre for Data Ethics and Innovation. This is the first body of its kind to be established anywhere in the world and represents a landmark moment for data ethics in the UK and internationally. The UK already benefits from a world-class regulatory regime, and the Centre will build on this by making sure we understand and respond to the rapidly evolving way in which data is impacting our lives. The Centre will identify the measures needed to strengthen and improve the way data and AI is used. It will operate by drawing on evidence and insights from across regulators, academia, the public and business and translate these into actions that deliver direct, real world impact on the way that data and AI is used. This will include articulating best practice and advising the Government on how to address potential gaps in our regulatory landscape. The Government has recently commissioned the Centre to study the use of data in shaping people's online experiences, and the potential for bias in decisions made using algorithms.

1.3 The Cabinet Office and DCMS are not alone in making progress in the fight against fraud

In addition to the initiatives of Cabinet Office and DCMS, there are a number of other initiatives across Whitehall working on using their data to counter fraud. Examples of some of these initiatives have been included in the contributions documented after p.15 in this paper.


Remote Admin
Malware
Identity Theft
Phishing
Hacker
Backdoors
Password
Crime
Virus Computer
Spam
Social Network
E-Commerce
Worms
Internet Scam
Username
Skimming

2. Key challenges to making even more progress

In recent years this Government has made great progress in the use of data analysis to counter fraud, as described in section 1. Unfortunately there are several key challenges we face that may inhibit this progress.

We are seeking your input on these points, from your observations of your own industry. We have included at the back of this document (p.71) a form for you to use if you choose to do so.

2.1 Data Mindset

Having a data mindset is about individuals in an organisation having an understanding of the value of data. This impacts the way policies and processes are designed; improving how and what data is captured and drives the development of better strategies, such as countering fraud.

Private sector and industry see the development of a data mindset as being key to the way businesses operate today.

Q1. Should the Government embed a Data Mindset, and how could it achieve this?

> "We believe that the latest technological developments and their applications provide another timely opportunity to achieve further, significant reductions in public sector fraud and error."
>
> Capgemini

2.2 Data Quality

We know that high quality and consistent data is key to making data driven decisions. This includes capturing data reliably and having a clear and consistent understanding of what any stored data actually represents. DCMS are working with departments across government to look at their data quality issues more broadly and consider what can be done to improve Government data. The Counter Fraud Centre of Expertise has developed a set of common data specifications for key counter fraud datasets to enable other organisations to engage with the data owners more effectively.

Q2. What should the Government do to improve Data Quality, and should it seek to develop standardised counter fraud datasets that can be consistently used and understood?

> "Ensuring Data Quality comes with a series of challenges (both technical and ethical) including, but not limited to, the following:
>
> - The means and processes through which the sources of data will be vetted, (bearing in mind that, among legitimate data sources, no single source contains all correct information and that not all information available is updated);
> - The jurisdictions and regulations governing different data sources;
> - The means and processes through which decisions can or should be made on what will ultimately constitute the official version of the data
> - The moral and ethical limitations of how that data will be used equally by the Government, business, or the citizens themselves."
>
> Dr. Georgios Samakovitis MEng, MSc, MBA, SFHEA

2.3 Data Capabilities

Analysing data and generating insights relies on having the appropriate analytical tools and then applying fraud relevant skills and techniques to distil insights and identify potential fraud threats. To date the Government has created a counter fraud analyst community to share knowledge and build broader capability. We also see in the private sector greater spread of data capabilities. As some tools become easier to use, it is a natural step for staff to self-serve or embed some of the data capabilities into their day to day working.

Q3. What more could be done to improve the tools staff have access to; as well as ensuring that they have relevant skills and capabilities to generate maximum value from using data to reduce fraud?

> "Analysis of High Performers in using data and analytics shows that High Performers have three times the level of top leadership and board commitment compared to those classified as Low Performers (89% vs 37%)"
>
> Accenture

2.4 Data Access

At its heart, using data and analytics to counter fraud necessitates accessing and sharing data between parties; whether that is a form of bulk sharing or on a case by case basis. The Government has worked to facilitate this by passing the DEA and through developing a Best Practice Guide. We see benefits in the private sector working with Government to enable data sharing to counter fraud in key sectors such as Car Insurance. Other technologies such as distributed ledger or blockchain could provide opportunities for Government departments to share data without the need for continually re-requesting it.

Q4. What should, and could the Government do to improve access to data in order to counter fraud in an economically viable way?

> "Fraudsters don't restrict their targets to a single organisation or sector (as evidenced by Cifas members obtaining most benefit from matching against data shared by organisations outside of their own sector) and therefore organisations can't afford to hold data within silos. Through this approach, Cifas members prevented fraud totalling over £1.4 billion pounds in 2018"
>
> Cifas

2.5 Data Ethics

For the public sector it is essential that use of data for counter fraud purposes is used ethically and within the existing legal frameworks. Whilst the use of data and Artificial Intelligence (AI) has the potential to enhance our lives in unprecedented, powerful and positive ways, we recognise that the issues in relation to data use and AI are complex, fast moving and far reaching. This is why we have established the Centre for Data Ethics and Innovation. Our businesses, citizens and public sector need clear rules and structures that enable safe and ethical innovation in data and AI - the Centre will recommend the measures needed to build trust and enable innovation in data-driven technologies.

Q5. To what extent should the Government seek to exploit the opportunities that emerging technologies like AI could provide in countering fraud, and what frameworks should be put in place to ensure their usage is ethical?

> "TransUnion commends the Government's leadership on data regulation and guidance on best practice use – particularly it's proactivity in creating the Data Ethics Framework in 2018, active membership in the EU's eIDAS knowledge and learning programme, as well as the recent appointment of the first national data guardian for health and social care. Projects set up under structured guidance have already shown promise. We see that creating a forum within a defined CUG (closed user group with defined sharing purposes) can lead to great benefits – a key reference point is the Cabinet Office-led National Fraud Initiative; an example of where specified anti-fraud organisations could have a role to play in supporting public sector on shared data projects."
>
> TransUnion

3. Your Voice

The aim of this paper is to spark a conversation with our key stakeholders: citizens, Government, industry, and academia; on the use of data analytics in counter fraud. We have laid out five key challenges that we have identified as barriers to further development in this area.

We recognise that answering some of these questions, and answering the ones we don't yet know to ask, requires we look inside and beyond the Government. We would greatly appreciate any insights you could provide based on your own experiences or observations in you industries.

1. Should the Government embed a Data Mindset, and how could it achieve this?
2. What should the Government do to improve Data Quality, and should it seek to develop standardised data sets that can be consistently used and understood?
3. What more could be done to improve the tools staff have access to; as well as ensuring that they have relevant skills and capabilities to generate maximum value from using data to reduce fraud?
4. What should, and could the Government do to improve access to data in order to counter fraud in an economically viable way?
5. To what extent should the Government seek to exploit the opportunities that emerging technologies like AI could provide in countering fraud, and what frameworks should be put in place to ensure their usage is ethical?

We also welcome any other feedback or thoughts you want to share with us on the issues discussed in this paper.

3.1 How to share your comments and ideas

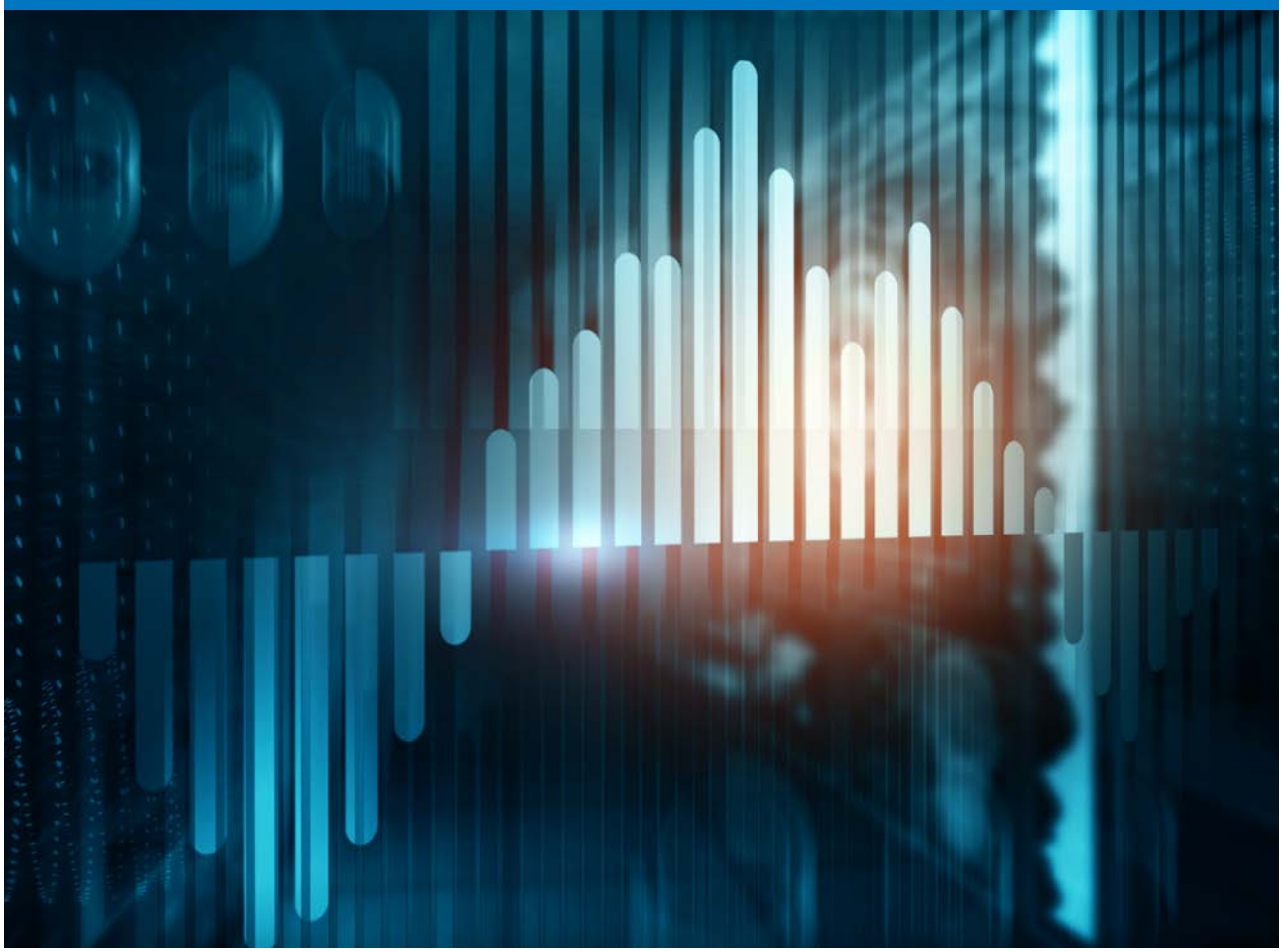
We have provided a form at the back of this document (p.71) where you can enter your feedback. Additionally there is an online survey available here.

Please email your responses to fraud.data@cabinetoffice.gov.uk or send them to us at:

Counter Fraud Centre of Expertise
Cabinet Office
70 Whitehall
Westminster
London, SW1A 2AS

Reference Contributions

We have included, verbatim, the contributions of the government organisations, academic institutions, and private sector companies that were consulted during the creation of this paper.



Contribution 1. UK Government

Cabinet Office

1.1 Cabinet Office

1.1.1 The Government Counter Fraud Function

What is the Government Counter Fraud Function?

The UK Government has taken a proactive approach to addressing fraud, focusing on building capability in public bodies to detect and respond to fraud risks through the establishment of a cross government Counter Fraud Function; one of fourteen recognised functions across government.

The functional model[6] was designed to move the Civil Service to the next stage in its evolution by breaking down the organisational silos staff had been held in, helping government departments to become even more effective at what they do. Over the past few years the Government has begun to strengthen the fourteen identified functions.

By connecting the 10,000 public servants working to find and fight fraud across the public sector, the Counter Fraud Function is breaking down silos in government's work and enabling the development of common standards. This will enable us to build stronger capability, to equip staff to understand their fraud risks and how best to respond to them, and to allow public bodies to draw on the best staff possible with assurance of the quality of service they are receiving.

What does the Government Counter Fraud Function do?

The Government functions cover common activities that run across departmental boundaries, with each undertaking a set of activities under the functional taxonomy in order to drive better outcomes. For the Counter Fraud Function these are overseen by the function's centre in the Centre of Expertise for Counter Fraud, in the Cabinet Office. These activities are:

- Developing capability
- Giving expert advice
- Driving continuous improvement
- Developing and delivering services
- Setting cross-government strategies
- Setting and assuring standards

6 "The functional model: a model for more efficient and effective government": https://www.gov.uk/government/publications/functional-model-for-more-efficient-and-effective-government

1.1.2 The Centre of Expertise for Counter Fraud (Cabinet Office)

What is the Centre of Expertise for Counter Fraud?

The Centre of Expertise for Counter Fraud sits at the centre of the Government Counter Fraud Function. It is a team of counter fraud experts, drawn from across government, who lead on the development of the function; bringing together and coordinating its work.

What does the Centre of Expertise for Counter Fraud do?

- Provide an evidence base for fraud in the public sector.
- Review cross-government compliance with the Government Counter Fraud Functional Standards.[7]
- Help public bodies develop action plans and metrics to fight fraud.
- Manage the Fraud Measurement and Assurance (FMA) programme.
- Build cross-government capability through the Government Counter Fraud Profession.
- Collaborate with international partners through the International Public Sector Fraud Forum.
- Develop the use of data and analytics to fight fraud in the public sector.

Using data and analytics

In addition to driving the Counter Fraud Function, the Centre of Expertise runs two analytical services that engage directly with public bodies; helping them to use data analysis to find and fight fraud. These are the Data Analytics Development Team and the National Fraud Initiative.

The Data Analytics Development Team run data sharing pilots with and between public bodies, providing project management and analytical expertise. Their proven approach is based on Best Practice Guidance developed with experts from the public and private sectors, to help government counter fraud teams employ data analysis more effectively in their work. They also oversee the operation of the Digital Economy Act which can enable the sharing of data to fight fraud.

The National Fraud Initiative (NFI) is an operational data matching service run from the Cabinet Office that works with public bodies, including Local Authorities, to help them identify fraud in their operations. Between 2016 and 2018 the NFI, in partnership with Synectics Solutions, helped its partners find over £300m of fraud, winning an Insurance Times Award for Excellence in Technology in 2018.

7 Cross-Government Fraud landscape Report 2018 - Functional standards for counter fraud, p.27: https://www.gov.uk/government/publications/cross-government-fraud-landscape-annual-report-2018

1.1.3 What next?

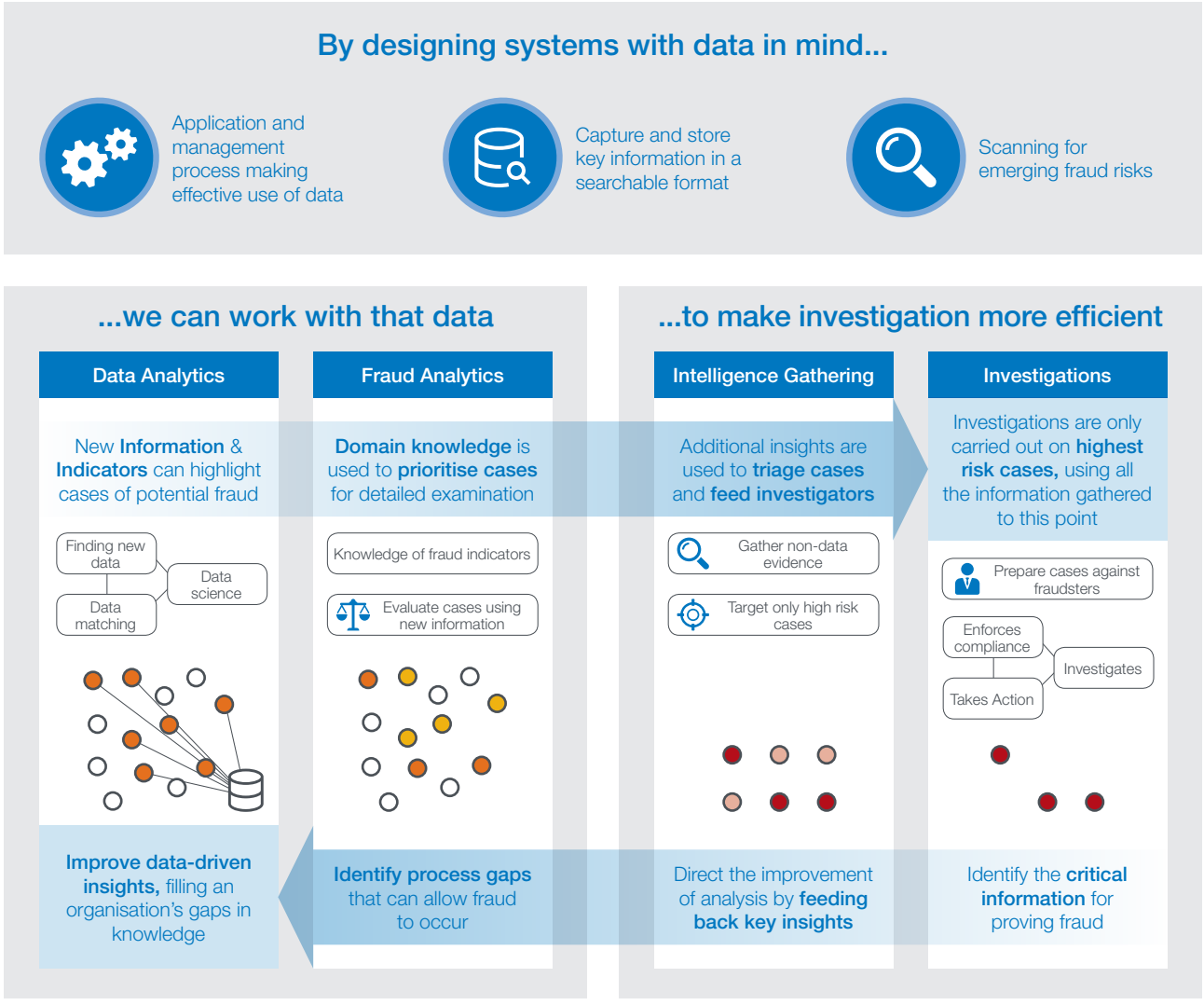
Historically Government's counter fraud responses have been reactive; focused on gathering intelligence and investigating low volumes of high value cases. These cases were often identified through whistleblowing or random sampling. The introduction of data analytics equips Government to take a more proactive approach to counter fraud.

Government already makes great use of intelligence gathering and investigation to take action against fraud.

Whilst investigations **must be the final stage** of counter-fraud work, they are resource intensive and have a significant impact on the public. Data analysis provides a scalable means of detecting and evidencing fraud, allowing investigations to be targeted more efficiently; increasing fraud recovery for any given cost to the taxpayer.

Employing data analytics allows **continuous improvement of fraud detection** by allowing key insights to pass from investigators back to analysts. Once developed, analysis techniques can be applied at the application stage; allowing organisations to work pro-actively to **prevent fraud.**

Figure 1 - Integrating data analysis into counter fraud strategy



Data analysis can collect and assess large amounts of highly varied information to search for indicators of fraud. It can be carried out on large numbers of cases, at a low per-case cost. These factors allow organisations that use data analysis to search through entire caseloads, rather than small samples of them, to identify high-risk cases. The result; using data to manage case referrals means that high cost and high impact actions like investigation and audit are only carried out on cases that are at high risk of fraud. This enables more efficient utilisation of those high cost resources whilst minimising their impact on citizens.

In considering what the next steps for integrating data and analytics into counter fraud strategies should be the Cabinet Office has sought input from Government, industry, and academia. These inputs have been included verbatim in this paper, but can be summarised as:

> There is an opportunity to shift Government from high cost investigations to lower cost interventions through the extended use of data and analytics.

Department for Work & Pensions

1.2 Department for Work and Pensions

DWP has developed its Fraud and Error Detection and Prevention strategy which puts the use of data and intelligence at the core. We recognise the importance of being able to access data and intelligence from outside of the Department in order to reduce claimant errors and minimise the chances of people being able to commit fraud.

We have an excellent track record in sharing and legally obtaining data, but challenges remain, particularly in regard to accessing financial data which might help us in tackling long standing issues such as undeclared capital, undeclared income and undeclared financial links between people (undeclared partner fraud or collusion between employers/landlord and claimants). We are intending to launch a public consultation in 2019 around widening data sharing legislation to help address this, and so we'd be looking for the work of Cabinet Office to complement and help position that consultation.

HM Revenue & Customs

1.3 HM Revenue & Customs

HMRC is a unique Government department bound by its duty of confidentiality given that it is only allowed to share information where a valid information sharing gateway exists.

HMRC has substantial capability to capture and use data to counter fraud through its Connect and Feast systems, and is driving the take up of the use of AI both in decision making and through the use of robotics on the processing of data.

The new fraud provisions in the Digital Economy Act (DEA) 2017 has helped to unblock some data sharing agreements to help combat fraud but the threshold to share data under these provisions is set a very high. Under the DEA, we are seeing an increase in the number of requests for Data sharing and invariably this will involve HMRC data (particularly RTI). Data Analysts are a very sought after commodity and we would wish to work with the Cabinet Office on approaches that will help alleviate and resolve this issue whilst satisfying the increasing demand for data to counter fraud.

1.4 National Economic Crime Centre, National Crime Agency

A large opportunity exists in the exploitation of fraud data for law enforcement. However, the sheer scale of fraud data is currently a barrier to fully exploiting the data. Better data exploitation and sharing will enable the NCA to uncover more criminality buried in the data.

The NCA ambition is for a national data exploitation capability, making data more available for the wider law enforcement system, complimenting regional work. Law enforcement partnership is key, leverage capability for a shared endeavour, with reuse for speed of reaction.

Using the powers vested in the Agency by the Crime and Courts Act to link together, access and exploit data held across government, the NCA is uniquely placed to act on behalf of the whole LE system. Automation is needed to identify risk and for target discovery due to the scale and complexity of fraud data available. This requires new skills in the workforce.

There are significant barriers to data exploitation around legislation and risk management. Legal issues impact the ability to hold and share data, and policy changes to risk management are potentially needed to direct resources from reported crime to the address the highest harm.

Public consent and concerns around law enforcement data collection are important and will need to be addressed as Law Enforcement builds capability in analysis of large scale datasets. Here, child sexual exploitation and abuse examples on the use of data to solve crime demonstrates a case of necessity. The scale and growth of fraud necessitates a growth in data analysis. However, the NCA is committed to a proportionate response, with analysis targeted on a small percentage of actors in datasets who demonstrate criminal activity.

Contribution 2. Case Study

2.1 Insurance Fraud Bureau - Why sharing data and analytics are needed to solve some problems

2.1.1 Background

The insurance industry has for a great number of years invested heavily in controls to prevent and detect fraud. Historically much of the fraud was viewed as being opportunistic in nature and that suited itself to manual controls. As the industry controls matured, those working within the industry perceived that there was an element of fraud that was not opportunistic but far more organised in nature.

2.1.2 The problem

Insurers and their supply chain observed an increase in claims arising from road traffic accidents where there were concerns about the validity of both the initial accident and the claim that followed. Anecdotally individual investigations were identifying that some of the accidents, were not in fact accidents at all, but were instead purposeful collisions between vehicles, designed to enable fraudsters to make fraudulent claims in a variety of way, not just relating the vehicle damage but for claims that may arise also following a collision such as cost of hire vehicles, whilst the damage is being repaired and also personal injury.

The concern was that those individual claims that insurers were looking at in isolation were not individual opportunistic frauds, but part of a much larger conspiracy.

2.1.3 Data sharing and analysis to solve problems

Given the perceived potential scale of the problem, insurers agreed that a different approach was needed and that trying to investigate the issue in traditional and largely manual ways would simply not work. The hypothesis was that if the industry pooled their data together, that they would;

- Be able to see the full scale of the problem, revealing the links between the claims that the fraudsters were trying to hide
- With an improved understanding of the scale and nature of the problem, be in a stronger position to tackle it

2.1.4 The solution

The model that has now been created is as follows;

- Insurers share claims and policy data with the Insurance Fraud Bureau (IFB)
- IFB take weekly feeds of the claims and policy data and ingest that into its analytics engine
- The system is designed to flag suspicious patterns and networks of behaviour
- IFB then have teams of analysts to verify the findings from the systems
- Only those networks that have been flagged by the system and subsequently verified by an analyst are pursued
- This analysis and intelligence development work, then enables suspect activity to be developed with a controlled number of subject matter experts within the industry

2.1.5 Benefit to society

As a result of pooling the industry data, it has been able to far more accurately estimate the scale of organised motor insurance fraud, with the latest numbers illustrating that the cost is in the region of £350 million per annum. The financial cost is not insignificant but the operational activity that has followed the data sharing and analysis has revealed that the harm to society is far graver than the financial cost alone;

- Many of the organisers of these types of scam are organised criminals involved in a range of other criminal activity alongside the insurance fraud
- The method of these scams includes the fraudsters taking vehicles out onto public roads and forcing unsuspecting motorists into collisions. These collisions leading to injury and in extreme cases loss of life

Since the IFB was created in 2006 adopting these methods has led to over 1245 people being arrested and 636 subsequently being convicted. Those convictions have seen custodial sentences exceeding 554 years and over 32,000 hours of community service.

Contribution 3. Fraud Solution Providers

3.1 Accenture – Use of Data and Analytics to fraud & non-compliance

3.1.1 Introduction

In today's fiscal environment every penny that governments have makes a difference, yet we know that fraud and non-compliance threaten to syphon off public funds and impact the delivery of public services.

From our work with Health and Public Service agencies around the world, we see an ongoing trend to make greater use of data and analytics to address fraud, risk and non-compliance. Whilst the early focus may have been on identifying and correcting non-compliance after transactions had completed, in recent years we have seen a shift to using advanced analytical insight to stop non-compliant transactions in their tracks, embedded as part of business processes and supporting a shift in focus to very much one of prevention[8].

We see that citizens' expectations of government today are very much the same as those for private companies and in the same way as we expect banks and financial institutions to deploy the latest tools and techniques to protect us, so we expect the same from government agencies.

By identifying and preventing fraud before the transaction is complete and focusing in on anomalies, agencies achieve direct savings in terms of losses and also free up the time of investigators and fraud teams to focus on the most complex and costly cases.

As has been highlighted there are a number of challenges that should be considered and addressed if the usage of data and analytics is to be successful:

3.1.2 Data Quality[9]

Data is the lifeblood of analytics and accurate information is essential to running any type of fraud models. Unverified or inaccurate information can have potentially serious implications for agencies and the risks need to be proactively managed and mitigated to ensure the integrity and veracity of data.

Our 2018 Technology Vision[10] brought some of the challenges to life:

- 82% of executives responding to our 2018 Tech Vision survey report their organisations are increasingly using data

8 https://www.accenture.com/no-en/~/media/Accenture/Conversion-Assets/LandingPage/Documents/1/Accenture-Raising-The-Performance-Of-Revenue-Agencies.pdf
9 https://www.accenture.com/gb-en/insights/strategy/data-quality-competitive-advantage
10 https://www.accenture.com/gb-en/insight-technology-trends-2018

to drive critical and automated decision-making, at unprecedented scale.

- 79% of executives agree that organisations are basing their most critical systems and strategies on data, yet many have not invested in the capabilities to verify the truth within it.

The good news is that existing tools and capabilities provide the power to address data quality issues and ensure the data integrity and veracity needed on which decisions can be made. The challenge is more likely to be around building a consensus and the buy-in to address the data quality in the first place.

Addressing data quality typically starts with a data audit that can help identify issues which need to be fixed as well as starting to quantify some of the value that improving data quality could have. Data quality standards and data handling standards can be developed to ensure that organisations have in place the tools needed to maintain the quality of this key business resource.

When looking at data quality it is also important to consider its various facets:

- Ingestion & content: Bad data collection, inadequate quality checks, and lack of system integration.
- Architecture & storage: Errors in database setup and storage processes result in unusable or mismatched data, such as missing customer IDs or unreliable records.
- Model & reporting risk: Analytic research and reporting conducted on suspect data will lead to untrustworthy operational and strategic decisions.

That said, when it comes to Data Quality trying to achieve "perfection" can be the enemy of done, and we need to remember that the value comes from using the data to prevent fraud and risk. Therefore, Government should look ensure it takes a pragmatic view of understanding the key datasets that need to be accurate and complete and focusing here, rather than getting lost in an attempt to resolve everything.

3.1.3 Data Mindset & Skills

By unlocking and sharing actionable data insights, organisations can become more agile, optimising customer decisions, prioritising fraud actions and better aligning finite resources. In order to do this, however, a new Data Mindset and set of Data Skills are needed across the organisation and in the way that people work.

In addition to recruiting data analysts and data savvy resources, starting to think about data as an asset requires a real mindset shift for most organisations. For an agency to move from being a passive collector to active analyser of data—and be truly data-driven—it must change the way it thinks.

An organisation's ability (or inability) to move to this way of thinking is, in our view, primarily a cultural issue, with many organisations underestimating the need for—and the scope of—the necessary cultural change. Our experience shows that when change management is undertaken, it is often done on an ad-hoc basis and as light touch, instead of strategically and thoughtfully. Whereas technological constraints once defined the pace at which analytics could innovate and grow, people are now finding that it is the organisation's own capacity for change that inhibits their ability to deliver at speed.

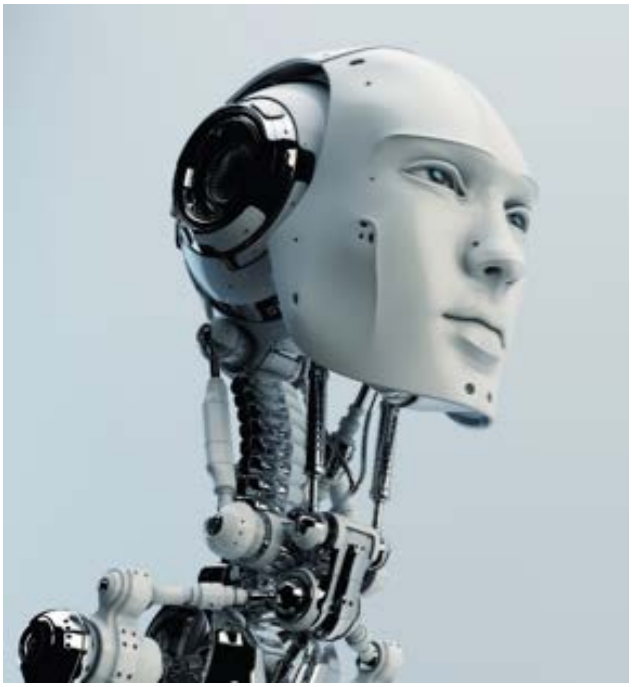
Key to getting this to stick is by engaging senior leadership and stakeholders: Our analysis of High Performers in using data and analytics shows that High Performers have three times the level of top leadership and board commitment compared to those classified as Low Performers (89% vs 37%).

In becoming a High Performing organisation we talk of the 5 A's of Analytics Transformation[11], the first step of which is Align. This involves leaders embracing the data mindset and the vision of what can be achieved through greater use of data. This can then help drive interest, engagement and involvement across the organisation.

Once this Alignment is in place, groups can start to move through the subsequent phases of the 5A's of Analytics Transformation, one of which is Adoption where stakeholders are engaged and involved in moving to the new ways of working.

Successful delivery of analytics insights and creation of long-term value

Align	Align Leaders and Build the Organisation
Act	Initiate the Analytics Journey
Adjust	Course Correct for Long Term Success
Adopt	Implement New Data, Technology and Expertise
Adapt	Decision Making Powered by Analytics



3.1.4 Use of Artificial Intelligence

Much is made of Artificial Intelligence (AI) as the new paradigm for data and analytics and changing the way in which humans work with machines. AI, is no longer just for hobbyists and academics looking for a challenging problem to solve. AI has gone mainstream with more and more adopting Machine Learning and more advanced AI techniques to analyse their data. This is not accidental. Since the early days of its study, AI techniques have steadily matured and grown in sophistication. As hardware, processing power and storage capacities have rocketed, so has the ability of organisations to solve complex, real-world business problems through the application of AI techniques and algorithms.

In the area of fraud and risk, the ability to use AI to solve complex issues, to make sense and drive insight from unstructured data and new data sources and keep fraud and risk models updated and accurate has the potential for game changing results. Yet in reality we see many organisations only making tentative steps.

11 https://www.accenture.com/t20161201T011012Z__w__/us-en/_acnmedia/PDF-33/Accenture-Analytics-The-5As-Of-Analytics-Transformation.pdfla=en

One key impediment to the adoption of AI is how to trust a particular model or algorithm when the result has been developed by what is inevitably seen as a "black box." In Financial Services this question is consistently posed by their regulators as well as by their own control functions such as model validation or internal audit and the same will be true for Government. The ability to explain the conceptual soundness and accuracy of AI techniques is a significant challenge, not only because the tools are so new, but also because many of the algorithms themselves are complex and difficult to explain.

AI absolutely plays a key role in fraud and risk detection as is fundamental when using some unstructured and new data sources, yet its usage goes hand in glove with a key focus on Data Ethics and explainable AI.

3.1.5 Data Ethics[12]

For AI to deliver on its promise it will require predictability and trust. These two are interrelated. There is a need to ensure that the complex issues addressed by AI lead to a level of predictability and consistency in treatment and results. Similarly, progress with AI requires consumers to trust the government's use of the technology, and the fairness of how they are affected by the outcomes.

A robust legal framework will be needed to deal with those issues too complex or fast changing to be addressed adequately by legislation. But the political and legal process alone will not be enough. For trust to flourish, an ethical code is equally important.

The government should encourage discussion on the ethics of AI, and ensure all relevant parties are involved. Bringing together the private sector, consumer groups and academia would allow the development of an ethical code that keeps up with technological, social and political developments.

Government efforts should be collaborative with existing efforts to research and discuss ethics in AI. There are many existing initiatives which could be encouraged, including the Alan Turing Institute, the Leverhulme Centre for the Future of Intelligence, the WEF Centre for the Fourth Industrial Revolution, work being done by the Royal Society, and the Partnership on Artificial Intelligence to Benefit People and Society.

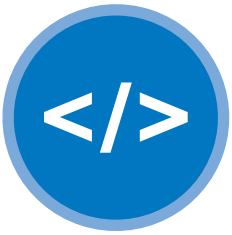
As more work is done in this area, there are opportunities to foster a public discussion to help build a set of fundamental ethical principles for AI development and data usage. Making those efforts inclusive, rather than exclusive or isolated, is desirable.

12 https://www.accenture.com/gb-en/company-responsible-ai-robotics

Set up an AI Advisory Body: To consider ethical issues, foster discussion forums and publish resulting guidance to the industry and regulators. Communicate developments to the public to show initiative.

Gather intelligence on and participate actively in the development of such codes internationally: The "Asilomar AI Principles" and the "Partnership on AI" codes should be considered, among others to pick up on the latest thinking.

Develop core ethical principles: Engage with stakeholders to put together and publish fundamental ethical principles.



Encourage the development of sector specific codes: Particularly in fast moving areas, as mentioned above.

In conclusion, government agencies have the potential to make use of the significant amounts of data which they process, whether this is around the transactions they complete, the people they serve and the programmes they develop. Yet data is just data unless Government knows how to act on it and extract value. This demands a steady focus on the outcomes being delivered, in this case a reduction in fraud, an ability to harness the power of technology rather than be limited by it, and a willingness to connect with leaders and wider stakeholders in new ways.

The real game changer in converting analytics into outcomes for fraud and risk is getting data insights quickly into the hands of those who can prevent and stop fraud from happening and helping UK Government protect the public purse.

3.1.7 About Accenture

Accenture solves our clients' toughest challenges by providing unmatched services in strategy, consulting, digital, technology and operations. We partner with more than three-quarters of the Fortune Global 500, driving innovation to improve the way the world works and lives. With expertise across more than 40 industries and all business functions, we deliver transformational outcomes for a demanding new digital world.

3.2 Atkins – Data sharing for public good

ATKINS

3.2.1 Data Sharing for Public Good

Imagine a country where government and industry share data in such a successful way that people are confident in getting the best medical and surgical outcomes; investments in infrastructure drive environmentally friendly industrial growth while reducing people's stress and promoting health; everyone who needs support because they've lost their job gets appropriate benefits in a timely way; every child gets a school place at the school that suits them the best; every family in need of help gets allocated a social worker to support them at just the right time; and funding flows through to all the places that genuinely need it. That funding gets spent on things that evidentially make a positive impact. But however idyllic that might sound, there are interesting cultural and technology challenges to this vision of nirvana.

3.2.2 Making it OK to share data

It can be remarkably difficult to share data across government. An early hurdle is simply identifying the legal framework to enable it. The law seems almost contradictory with the General Data Protection Regulation (GDPR) promoting a culture amongst data guardians where it's safer to say no. Those wanting to share data need to make a good case to do so. By contrast the Digital Economy Act has at its heart a premise of the opportunity there if the data can be unlocked. There's a tightrope to be walked between these two and amongst various other legislation relevant to the data specific to any given situation.

Atkins has supported government to design a range of data sharing software. We've also worked to understand and sometimes help to put into place the legal frameworks that support that data sharing. These frameworks are important and set the background for guidance and mandates on the use of cross government data sharing software. For example, it seems obvious now that parents should be able to apply for Free School Meals online. But it took an enormous amount of work from a blended team to enable the benefits data that underpins eligibility to be shared with the Department for Education (DfE). There's sometimes a public assumption that government data are government data. If someone is claiming a benefit from the Department for Work and Pensions (DWP) then it shouldn't be too hard for DfE, for local authorities, for schools to know about that. Admittedly - when there is a case for the public good the legal gateways are usually there or accessible. But it's not nearly so obvious to set up as you might assume without a closer look.

Add into this the technical difficulties of designing and building the software and infrastructure to get that right. And of course, the huge job of change management to get those delivering the services to change what they do and how they do it. Not to mention getting citizens to log in and use the online version of the service if it's citizen-facing. Government has no option to target its services towards the most lucrative market in the way that private sector companies do. Equity of service is the only option.

When it works well, it works incredibly well and in the new world where the data sharing is operational, the thing that seemed so tricky to think about seems an obvious no-brainer. Of course, parents should be able to apply for Free School Meals online with government taking the responsibility to check against eligible benefits. Of course, with the creation of the new Counter Fraud Data Alliance, we should be able to share data about known fraudsters to identify where there is a heightened risk of fraud.

3.2.3 Our Natural Unease – and Surprising Recklessness

Our natural reaction to be being asked whether it's OK to share some specific data about ourselves seems to be to recoil away. There have been some false starts, with our unease about data sharing being a key factor. Atkins supported a project called ContactPoint. The intention was to share a minimum amount of data about children accessing services so that those with multiple interactions could be spotted and supported more easily. It seemed a rather obvious, if technically difficult, measure that government could take to facilitate earlier detection of cases with multiple data points that wouldn't previously have been joined up. But this project was halted. Public opinion supported the stopping of this project and there are some very rational reasons for this public reticence. But done well, there is huge benefit to effective data sharing. In this instance, the need for this kind of system perpetuated and government is introducing the Child Protection - Information Sharing project (CP-IS). Every reader will know of other, similar examples where our natural reticence as citizens to say "OK" to sharing data has meant that projects have got so far and then stopped. Sometimes only to have to be started up again. We contradict ourselves. If we take the example of the NHS, everyone wants more efficiency out of the NHS, but it is still built upon letters, faxes, siloed data. The citizen should not ask 'do I trust the NHS to have a centralised store of my health records' but 'if I am taken ill when away from home then how beneficial could it be if the professionals can access, under control, my health records.'

At the same time people were and are continuing to entrust more and more of their data to online private sector organisations. Many of us will share data abundantly if we're not asked specifically, or if we're asked so specifically we ignore the question. Websites now have to say they use cookies – either click here for vast amounts of impenetrable detail or just say yes. Most of us just say yes. People are willing to provide their data in return for benefits, (or perceived benefits), including access to information and social interaction. We are sharing all kinds of personal data with private companies and very often different types of data that could be consolidated, combined and used for more than just personalised advertising if anyone chose to do that.

3.2.4 Government and Corporate Responsibility for Handling Data

The fact remains therefore that clumsy use of data would undermine trust in public services. And where we're dealing with anything that requires any kind of interpretation it adds another layer of complexity. There's a concern currently about bias in Artificial Intelligence (AI). If an algorithm is deciding someone is more likely to be guilty of fraud, how can we check how it came to that decision? Can AI be charged with making decisions? Even if it only makes recommendations, is that still too far? How can we be certain that AI that learns in an unsupervised way is not just repeating and amplifying inherent prejudices?

It's incumbent on government and those working with government to treat data properly. This means thoughtful and complete application of data protection principles. This is more than just the obvious, restrictive rules e.g. how long we can store data, what purposes we can use data for. It extends beyond this to future-thinking the way we design our software, data gathering and databases for data sharing and analysis. Anyone working in the industry is familiar with the difficulties and complications we face with various legacy databases each doing important useful things, often with the same data. It can be easier sometimes to create yet another database – even if it seems better, for example because it's in the cloud. It's incumbent upon all of us working

in government and beyond to think through the impact and the subtleties of what we're designing. It's surprisingly easy to increase the risk of redundancy of data, the risk of accuracy or to create multiple versions of the truth.

3.2.5 Technologies to Support Fraud Detection

Counter fraud is an important subset of the government data sharing landscape. Atkins has worked closely with the Cabinet Office to help make the Counter Fraud Data Alliance a data sharing reality. This is a data sharing alliance between the public sector, banks and insurers. Government and industry work in partnership to securely share known fraud data for the prevention, detection and reduction of fraud. It started with DWP, HMRC, insurers and banks. The intention is for it to grow, covering more fraud problems, more business processes and more organisations.

3.2.5.1 APIs

A core technology for any data sharing is the use of APIs (Application Programming Interface). Put simply, this means that different technologies can use a common language to communicate specific information with each other. So instead of a human needing to input data at one end of a conversation, multiple technologies can each "talk" to a central hub in technology-to-technology conversation. APIs can make the transfer of data smoother, quicker and removes the chance for human error. They can also make the transfer of data unnecessary in some cases: one version of the truth can remain, with APIs querying a trusted, up-to-date data source. Designed and implemented well they can reduce the need for multiple versions of the truth, increasing data quality while being able to share data faster.

3.2.5.2 Distributed Ledger Technology (DLT) / Blockchain

Blockchain technology potentially takes things a step forward again. No-one yet knows what the impact of blockchain will be, but it is already changing banking. Instead of a centralised authority, a consensus mechanism between network members trades data securely across a distributed ledger that must stay synchronised, meaning there can only be one version of the truth. When any agency updates their own database, other members can be notified with rules set to control permissions and legislation defined in the code. A single notification of a change in data could mean that every agency or database that needs to know about that change knows instantly. Data across many different departments and agencies would be consistent and accurate. For counter fraud, this could mean a distributed set of authorised accounts with different permissions able to share data seamlessly. One version of the truth means higher data quality and the ability to share more data in near real-time. However, as for all sociotechnical security systems the users remain the weak link no matter how cutting edge the cryptography used and managing this risk remains paramount. Also, for Blockchain to be safe and secure, the infrastructure it uses must be resilient - and size counts.

3.2.5.3 Artificial Intelligence and Robotics

The rapid pace of development in Artificial Intelligence (AI) since 2012 represents the maturation of a technology that has existed for over 50 years and is set to bring further opportunity for improvement to identify and counter fraud. The convergence of large data sets, powerful hardware and advanced algorithms have made AI increasingly capable. First steps include faster data analysis. In the field of counter fraud, in its simplest terms, AI can search through vast amounts of data to look for patterns and identify potentially fraudulent transactions.

The clearer the rules, metrics and recognition features a task has, the higher the likelihood that a machine can be optimised to undertake the task with confidence. This is leading to surprising outcomes: roles traditionally considered to be challenging and that involve data sorting or deterministic analysis can be automated, and in time autonomous. Machine learning algorithms are not as good at understanding complex unstructured data such as images and undertaking non-deterministic analysis yet. However, machines are increasingly outperforming humans at aspects of some of these challenging tasks, including image recognition, bulk data analysis and providing decision options.

It's critical that parameters and regulations are put around automated and autonomous decision making, and the Digital & AI Ethics body is welcome progress here. Atkins has worked with AI, for example in running trials for Connected and Autonomous Vehicles (CAVs) and the Facial & Biometric Recognition system at Heathrow. In CAVs, the sensors, AI and Vehicle Rules Engine (effectively the CAVs brain) use a constrained neural network to assess the situation a CAV faces, using many types of data from sensors, as well as default programming and coding. As we move from CAV trials to CAV adoption and more open-road use, it's essential that as well as understanding the Highway Code, CAVs learn human driver behaviour and the decision-making criteria of other CAVs. We have seen examples of CAVs testing inbuilt rules as they develop awareness of road use, both travelling too slowly and too quickly. Sometimes the AI learns what's right by getting seemingly obvious things wrong first.

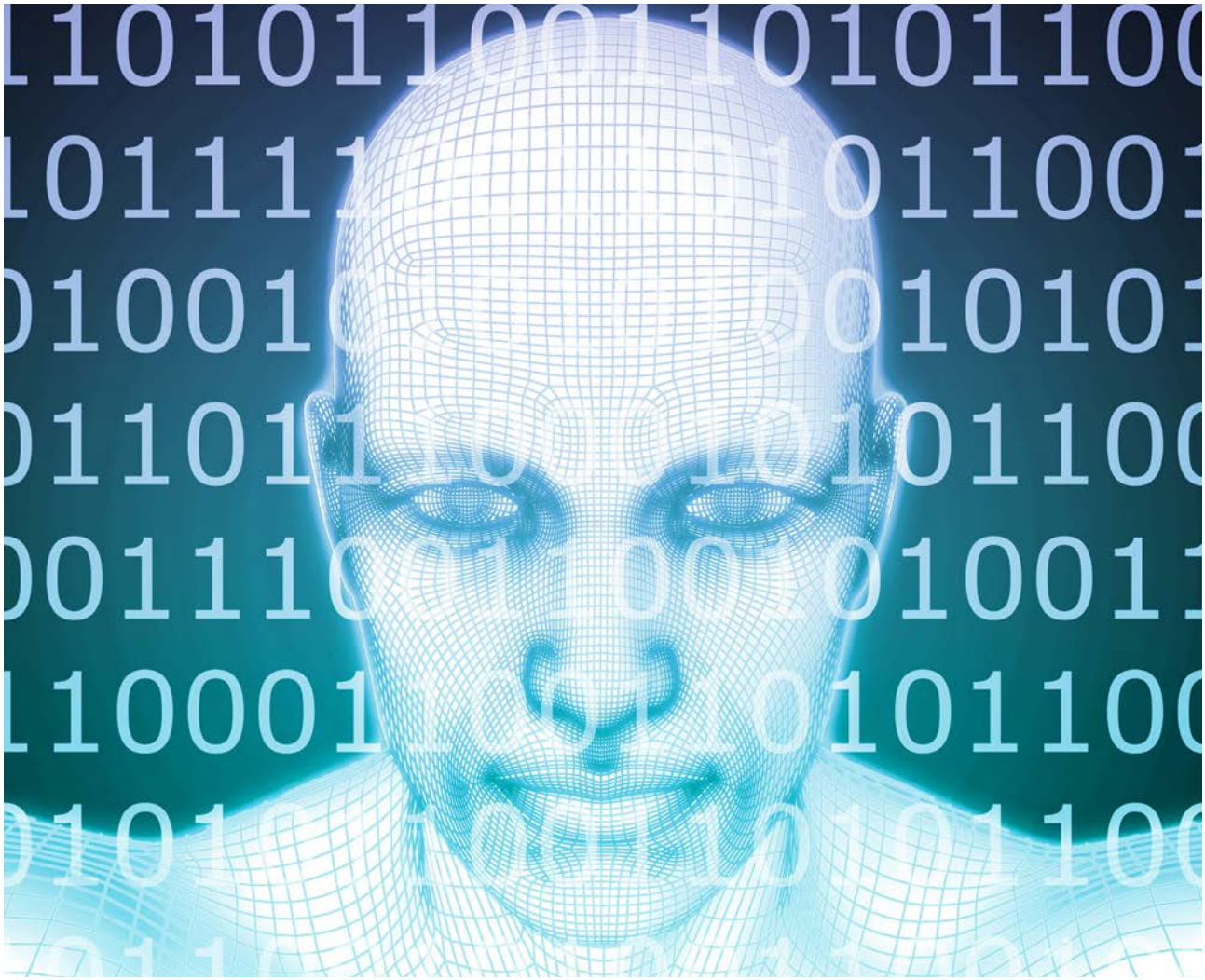
Sticking with the CAV example - at this stage, the deterministic and constrained neural networks help CAVs operate as single, autonomous entities with little or no human intervention. Scaling up will mean fleets of CAVs driving together and probably true unconstrained AI within and between CAVs. These will be non-deterministic which means current recognised safety and certification good practice cannot be applied and a new way of assuring and certifying safe use needs to be applied. Any application of AI needs to accept that the way we set parameters and regulations needs to adapt to suit the pace and potential of what we put into place.

The topic of AI being involved in decision making is central to its application in counter fraud. Certainly, AI promises quicker decisions examining a broader range of data. Particularly when human mental capacity is increasingly unable to cope with the data deluge. Optimising human and AI capabilities in teams that maximise strengths and mitigate weaknesses is essential. There are frequent claims it creates more accurate decision making (better than human), although in most areas, this decision-making is in its infancy. There is a lack of research examining how the use of algorithms influences human decision-making in practice and a recognition that bias can be introduced through reliance on historic data for comparison as well as the fact that potentially biased humans code the way the AI learns.

3.2.6 Regulation and Control

All of this points to the need for more research to be able to regulate and control AI whilst reaping the enormous benefit it potentially has to offer. There is so much more than just clever programming needed to make AI a success. Recognition of this need is becoming more mainstream. The EU recently published its seven principles for ethical AI. The Centre for Data Ethics and Innovation and the Cabinet Office's Race Disparity Unit are set to examine the potential for bias in automated decisions. Think tank the Police Foundation recently recommended that new regulations and practice should be developed on how algorithms are used in policing and criminal justice, pointing also to the fact there is a limited evidence base on the efficacy and efficiency of different systems, their cost-effectiveness, their impact on individual rights and the extent to which they serve valid aims. Another think tank, RUSI, recommended that limited, localised trials should be conducted and comprehensively evaluated to build such an evidence base before moving ahead with large-scale deployment of such tools.

Technology is developing fast and our key recommendation is that the research, advice and regulation that goes hand in hand with this technology needs to keep up. We predict – and hope for – a growth of peripheral services and technologies needed to support the core technologies.



3.3 BAE Systems – Challenges of Data Sharing within Government

BAE SYSTEMS

3.3.1 Background

BAE are a leading supplier of cyber, intelligence, and security capabilities to government agencies, and a growing supplier of cyber and network security capabilities to commercial customers.

Government Data has been held in silos for a long time, replicating the traditional binders and filing cabinets of offices of the past. Although data has become increasingly digital over the years, the storage and sharing approaches haven't kept pace, meaning data has continued to remain in silos, often far from where it could be more valuable. Fraudsters, for example, act by exploiting the gaps between these silos – deliberately misrepresenting themselves across multiple data sources safe in the confidence that they won't be found out. In the case of fraud detection and prevention, therefore, shared data brings its value by helping investigators build richer, more complete pictures on which to uncover suspicious activity after the fraud, but also by equipping organisations to build more robust preventative defences before the fraud. So why are there still challenges to data sharing?

3.3.1 Challenges to data sharing

a. Legislation - Historically, there has been a perception that legislation does not support or enable the sharing of data. While this has never been true – the DPA1998 included specific provisions under S29 enabling the sharing of data for the detection and prevention of crime – many organisations have continued to incorrectly hold this view. Recent legislative changes, including the Digital Economy Act 2017 and the Data Protection Act 2018, have further negated this challenge.

b. Perception - A more pressing challenge has been the perception of data sharing. Data sharing can encompass everything from aggregated data openly published on the internet (e.g. via data.gov.uk), through the use of anonymised, psuedonymised or personally identifiable information at a record-by-record basis, to the sharing of bulk datasets.

The usage of the shared data is important to understand what is proportional, and why in some cases (e.g. behavioural analysis for detecting insider fraud) it may be necessary to share bulk personal information, whereas in others (e.g. identity verification for credit card and insurance claim applications) it is sufficient to use API requests or tokenised data to share. Despite these varying uses, a common challenge is overcoming or mitigating the reputational risk associated with sharing data. Related to this is the difficulty in attributing benefits to the act of sharing data, which adds to the difficulty in justification.

3.3.2 Cyber risk

A valid and relevant concern which raises doubts around data sharing is the increasingly prevalent appearance of data breaches in the media, and the increasing volume of discussions in this area. This has served to raise the level of literacy in the wider public around data security but, understandably, has introduced a new risk to many senior officers and executives which, in many cases, still isn't fully understood. The fact that the National Fraud Intelligence Bureau is now the UK's National Fraud and Cyber Crime Reporting Centre shows how intrinsically these two domains are interlinked.

3.3.3 Skills and capability gaps

Although the challenges above do exist to commencing data sharing projects, they are often overcome relatively easily. More challenging is the difficulty in organisations to extract data from systems for sharing, or to build new extracts and APIs for automated data sharing. This can and does slow down the initiation of projects across both the public and private sector.

3.3.4 How have these challenges been overcome?

Some of the challenges above have been systemically dealt with – for example, new legislation has simplified the legal gateways for the sharing of data. The National Cyber Security Centre's proactive work in reaching out to businesses and providing more guidance has also led to increased understanding of what good information security looks like, and what organisations should demand of their suppliers and partners. In other areas, smaller scale solutions have been implemented which have the potential to expand and addresses these issues more widely.

3.3.5 A focus on outcomes

We advocate that organisations focus discussions on outcomes and, increasingly, we are seeing this in our interactions with customers and partners. A focus on outcomes and understanding what is trying to be achieved helps to explain and justify the need for data to be shared, and gives boundary to what might be deemed proportional to share. A focus on outcomes also ensures fairness in data sharing, and this is a fundamental principle of privacy.

Taken to its conclusion, this can lead to a significant shift in approach. We recently heard from a local authority which has developed a data sharing charter, which commits partners to sharing data by default, unless legal or ethical barriers exists, in pursuit of improved outcomes for the communities they serve.

3.3.6 Making distinctions between the different types of data sharing

Following on from this, a greater understanding of what is meant by 'data sharing' has helped break down some of the barriers, both real and perceived. Data sharing encapsulates a wide range of technical approaches from bulk data sharing, transactional API requests and data enrichment, through to data validation and verification. These approaches can all have different data requirements, and that granularity of detail has enabled organisations to find compromises that still allow outcomes to be achieved.

3.3.7 Understanding the power of non-personal data

While, typically, personal data is needed to drive operational tasking (e.g. better quality alerts and cases, fewer false positives, etc.), there are a number of areas in which non-personal data is extremely valuable. These include strategic insights (i.e. not operational tasking), predictive analytics, visualisation and policy and planning. Non-personal data can support better decision making.

3.3.8 Use secure cloud solutions

In the last few years, the adoption of secure cloud solutions provided by commercial organisations has increased. Coupled with changing attitudes, organisations are now more willing to use these solutions, which provide ease, interoperability and commonality amongst partners and suppliers. A highly advanced organisation in government on this front is the Home Office, which is actively looking at the use of commercial cloud provision at an enterprise level.

3.4 Capgemini – A Point of View: Combatting fraud and error through data science, collaboration and incentives

3.4.1 Introduction

"Our work for government and the wider public sector generally, is evidence of Capgemini's deep commitment to, and support for, the UK's public services." Christine Hodgson, Chairman, Capgemini's UK Business Unit.

The UK Government has intensified its efforts to reduce fraud and error in recent years, with a variety of targeted programmes across departments and agencies, building expertise and achieving some notable successes. There is now a much clearer understanding of the scope and scale of the problem, high risk areas have been prioritised, intelligence sharing has increased, there is a greater focus on prevention, and stronger enforcement regimes and sanctions have been applied.

Significant volumes of taxpayers' money have been saved or recovered, providing a welcome boost to the public finances. In addition, the updated Digital Economy Act is encouraging ethical data sharing, while the recently-launched Government Counter Fraud Profession will deliver an army of 10,000 public sector counter-fraud specialists. We believe the government can go further through using artificial intelligence, robotics and machine learning to streamline processes, spot anomalies and create actionable insight.

From Capgemini's perspective, as we help to deliver flagship programmes for a range of departments and agencies, alongside our extensive experience supporting market leading private sector organisations, we believe that the latest technological developments and their applications provide another timely opportunity to achieve further, significant reductions in public sector fraud and error.

Our collective ability to gather, interrogate and analyse data is now greater than ever, providing rich insights on which to build policy and process, and take direct action. There are more opportunities and platforms for collaboration across government than ever before.

And throughout departments and agencies there are already countless examples of data-driven excellence, bearing down on fraud and error – and improving services for citizens in the process.

3.4.2 Our Points of View

Capgemini believes that there is real potential to enhance trust in our public institutions, and save hundreds of millions of pounds, by focusing on three areas to further drive down fraud and error in the public sector.

Capgemini's Government Data Analytics Platform (GDAP) provides a framework to reuse and share existing assets, skills and services, through integrated analytics services.

Drive a culture change towards real time checks and prevention, rather than retrospective reviews and follow up.

Build a meaningful incentive model that rewards those that share data, as well as those that consume it in eliminating both fraud and error.

3.4.3 Capgemini's Government Data Analytics Platform (GDAP)

GDAP provides a framework to reuse and share existing assets, skills and services, through integrated analytics services Departments and agencies across government are already a rich source of data analytics expertise and assets - and all plan to further exploit the tremendous potential that data science provides.

- The Home Office's Data Analytics Competency Centre is playing a leading role in its transformation into a fully datadriven department.
- HMRC's PAYE system processes real-time data and has leading-edge analytical capability.
- Defra's data transformation programme is enabling ground-breaking digital innovation within the department and includes plans for a Defra Data Lab service.

We believe that, rather than building new services or one large centralised service, there are huge benefits to be achieved by establishing a shared repository of all existing public sector data science expertise and assets. This would enable a speedy and thorough assessment of the prospects for sharing and repurposing those proven solutions within other departments, their agencies and the wider public sector. As well as having the potential to fast track significant results in the fight against fraud and error, it will also help to prevent duplication of substantial effort and spend.

3.4.4 The Government Data and Analytics Platform

Capgemini's proposals for a Government Data and Analytics Platform (GDAP) provide a new model to meet these challenges head on, promoting inter-departmental collaboration, overcoming technical barriers and deploying proven expertise and assets (which are already saving millions of pounds). It will speed up citizen services, improve compliance with key policies and laws, and directly facilitate the many new systems needed to deliver the UK's exit from the EU, building in protection against fraud and error. GDAP brings together a range of capabilities and services that are already proven for three of the biggest central government departments and there is potential for it to be applied across all departments and agencies at speed. At its core is a catalogue of analytical tools compiled from departments, underpinned by a managed data platform and a central innovation lab, all available via secure, UK-based cloud hosting and delivered on a consumption basis.

Any proposal to increase data sharing brings with it added ethical and legal responsibilities to set and maintain world class data protection standards. This is all the more significant given the growth in the use of new technology such as artificial intelligence and algorithms to interrogate data and inform decision making. This has led to an increase

in the study of artificial intelligence ethics - a key component of any artificial intelligence or data science strategy. For example, how should government's legal and statutory responsibilities be executed if algorithms and artificial intelligence are driving decision making? Do bots need government clearances? Who is responsible if a bot makes a poor decision? Capgemini can help navigate this ethical debate.

In a nutshell, the UK Government must maintain the trust of citizens, that it is moving with caution, transparency and wisdom, with rigorous safeguards in place to protect privacy and security. We believe that GDAP provides a framework that will enable widespread data sharing, while meeting all ethical and legal obligations.

We look forward to exploring how GDAP can be fully embedded in the national effort to share and repurpose government data science and expertise in the fight against fraud and error.

3.4.5 Drive a culture change towards real time checks and prevention, rather than retrospective reviews and follow up

Since 2016 the National Fraud Initiative (NFI) has saved the taxpayer over £300 million by detecting fraud and error in the public sector (Cabinet Office, 2018). The recently launched Government Counter Fraud Profession is another positive step, delivering new standards, guidance and tools to help build capacity and capability in the form of 10,000 public sector counter-fraud specialists.

However, the work of the NFI is characterised by high volume, cross-referencing activities to retrospectively identify potential fraud, which is then targeted for clerical review and follow up.

While this has had success, it generates high volumes of labour-intensive clerical work at a time of squeezed budgets - and although fraud is pinpointed, and the necessary actions taken, recovering money is often much more difficult.

That's why we believe that with modern technology and enhanced artificial intelligence capabilities, government should look to update the NFI's focus, moving it into proactive mode, taking instant, real-time, preventative action against fraud and error, at both application stage and at key events like change of circumstances or payment. This can be achieved with minimal human intervention and eliminates, at source, the need for costly and time-consuming review and recovery.

Moving to a proactive approach requires a shift to a culture in which, at every stage, we are asking the question: "I am about to do this – is it safe?", rather than one in which we review decisions and actions after the event. In the financial services sector, the boom in online applications for loans, mortgages, bank accounts and credit cards has driven the development of automated technology and the application of artificial intelligence to provide lenders and brokers with instant access to the accurate data they need to process and deliver a fast decision, in the face of white-hot competition.

Customers value the speed of service and definitive outcome, while the financial institutions have met their commercial imperative and significantly reduced their risk by safely pre-qualifying applicants in real time – acquiring new customers quickly and cost-effectively, with minimal human intervention.

Real-time applications Utilising GDAP principles, Capgemini has successfully applied these principles in both public and private sector settings.

We have worked with Cabinet Office, HMCTS and HMRC utilising PAYE data to understand whether fraudulent means declarations, or errors, were being made in courts as part of the fine setting process for road traffic offenses. In principle, PAYE information could be made available to magistrates as part of the evidence submitted to the court, supplementing the statement of means provided by the defendant. If found guilty, fines are set based on the severity of the offense and an appropriate percentage of the defendant's income. Through data analysis we found that 35% of individuals submitted data containing fraud and/or error, 63% withheld earnings information and 9% of those declaring themselves unemployed were in fact employed. Armed with this information it was clear that 94% of fines could be more accurately calculated if PAYE information was available to the magistrate. And more accurate fines result in a greater likelihood of them being paid, eliminating the need to bring offenders back to court for non-payment, with all the associated costs and pressure on court time. In addition, Capgemini has provided agile, developer, and platform capability supporting the delivery of a real time service to assess the status, risk and compliance of people and freight approaching and crossing the UK border. Successful implementations of this service will assess tens of millions of pieces of information in real time against an assurance scoring platform. This will allow government agencies and organisations to spot potential victims of human trafficking, national security threats, and organised crime, allowing government officials to act on this information to support victims, secure the UK, and save significant sums of public money.

3.4.6 Build a meaningful incentive model that rewards those that share data, as well as those that consume it in eliminating both fraud and error.

As discussed earlier in this paper, there are a range of challenges to overcome to fully create the conditions in which secure, frictionless data-sharing across government becomes the norm. Historically, organisations making successful efforts to prevent fraud and error have been rewarded with the satisfaction of a job well done and the knowledge that taxpayers' money is being protected and used appropriately. This is the essence of the public service ethos that we at Capgemini value and admire.

However, new technology, the evolving legislative framework, and investment in counter fraud and error skills and capacity, are coming together to help create an environment in which the reuse and sharing of data science expertise and assets can become the norm, supported by a culture focused on real-time prevention, rather than review and recovery. But to fully capitalise on the opportunities that these developments have opened up, we believe that the next logical step is the introduction of a broad range of incentives that help to generate and reward excellence in counter fraud and error.

While incentive mechanisms are commonplace in the private sector, we do of course recognise that the landscape, priorities and financial drivers are different and more complex in the public sector.

However, we are confident that a robust and transparent model, featuring clearly identified, tangible and measurable incentives, can be created to engage and motivate all departments and agencies, enabling those organisations to benefit from making meaningful contributions to the campaign on fraud and error, and in turn the public purse.

By applying push and pull principles to this endeavour, data sharing and the many benefits that follow can be achieved more quickly, not only bearing down on fraud and error but also generating new income streams that reward those organisations - and those that use their services - for their data-sharing efforts.

3.4.7 Galvanising collective action

For example, if a department or agency required to reduce its spending by 10% had the prospect of offsetting that reduction by redoubling its efforts to reduce fraud and error through data sharing and collaboration, we believe that would provide a powerful incentive through which to achieve the behaviour change we seek.

Equally, if a local authority successfully clamping down on fraud and error – and sharing its data and expertise with neighbouring authorities – were to receive a boost to its hard-pressed budget for essential citizen services, everyone wins.

The model can serve to galvanise collective action, both at organisational level and across government, fostering motivation and an entrepreneurial spirit. It is important that central government organisations set up to oversee expenditure and investment in artificial intelligence and data science take a lead in this regard. The Spending Review and departmental annual budget processes provide the opportunity to build in incentives to work more effectively across government i.e. sharing data openly within a secure framework can be rewarded with additional funds. This, coupled with an inability to get large investment projects through central government review and approval systems, could transform cross-government data sharing behaviours overnight.

Capgemini has broad experience of creating new business and commercial models featuring incentives and we look forward to exploring the details of how a new and robust set of incentives can help drive the broad application of data science in the fight against fraud and error.

Capgemini welcomes the opportunity to explore these three themes with government as part of the strategic planning for SR2019.

3.4.8 About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organisations to realise their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

3.5 Cifas – What can be achieved by bringing fraud data sets together

3.5.1 Context and background

a. Cifas has, at the request of the Cabinet Office, developed this paper to inform a 'Thought Paper' which aims to demonstrate what can be achieved by bringing fraud data sets together.

b. Cifas has 30 years' experience of public-private fraud data sharing, preventing over a billion pounds worth of financial crime each year. Cifas is also a trusted provider of Government data sharing solutions, including the Counter Fraud Data Alliance, allowing DWP, HMRC, and the private sector to share fraud data. Cifas is therefore well placed to provide a view on the opportunities that data sharing provides to combat financial crime, and where opportunities are presently being missed.

3.5.2 State of play - progress and limitations

a. There has been significant progress in fraud data sharing in the past decade, particularly in the public sector, which had previously been hampered by the absence of the required vires for public-private and even public-public data sharing. This changed through the provisions within the Serious Crime Act, which enabled public sector organisations to share their fraud data with the private sector, and other public sector organisations, through a Specified Anti-Fraud Organisation (SAFO).

b. There are however public and private sector organisations which are either not sharing any fraud data outside of their organisation/department, or where the sharing is extremely limited in terms of scope and breadth of access. There are a variety of practical (e.g. resource, system limitations), cultural (e.g. risk appetite for data sharing) and other reasons (e.g. perceived legal issues) for this, but they must be overcome to reduce the billions of pounds being lost to fraud, and the harm caused by those frauds and the illicit funds generated.

3.5.3 More organisations sharing more fraud data, more effectively

a. Understanding and utilising the legal provisions - Some organisations claim that they cannot legally share data for crime prevention purposes, and that fraud data sharing of any kind is not legal. Clearly the legal provisions are there, and far from precluding data sharing, GDPR provides a framework for organisations to undertake and evidence the work required to ensure that their sharing is legal and transparent. Organisations need to understand and apply the law effectively and be brave: a shift in mind-set is required to seize data sharing opportunities and ensure that more of Government utilises and benefits from the available legal gateways.

b. Sharing more data, more widely - While proportionality is key to fraud data sharing, too often the perception and use of the term creates over-cautiousness and barriers to optimum data sharing. In many instances a small amount or sub-set of data is shared with a limited audience on the basis of 'proportionality', where there is clear justification to share more data sets and more entity information with a much wider audience. The key is ensuring that the right security, audit and access controls are in place – all data sharing should flow

from that point. Fraudsters don't restrict their targets to a single organisation or sector (as evidenced by Cifas members obtaining most benefit from matching against data shared by organisations outside of their own sector) and therefore organisations can't afford to hold data within silos. Through this approach, Cifas members prevented fraud totalling over £1.4 billion pounds in 2018.

c. Utilising new technologies in the fight against financial crime - As criminals evolve and utilise developing technologies to facilitate their crimes, so must practitioners keep atop developments to stay one step ahead. CFDA provides an example of a straightforward but valuable tool, and Cifas' own systems illustrate a more developed model of data sharing, matching and in-built analytics. But there is far more available and we must further develop fraud prevention and detection through AI, machine learning and enhanced analytics, to most effectively tackle fraud and overcome privacy challenges (for example, where the data shared must not be attributable).

d. Understanding the scale of the iceberg - If we limit the data we match, interrogate and investigate to only selected targets, based on assumed knowledge, then we'll fail to identify and understand the wider threat and, ultimately, will not be able to provide the most informed response. Put simply, we don't know what we don't know. Once a full fraud risk assessment is undertaken, organisations should use data to test their assumptions and tolerances, exploring where fraud may be uncovered, and where the effective use of data can be employed to identify, and limit, risk.

e. Full and effective deployment of data and data matching - Too often when organisations receive or match against fraud data, it is narrowly and ineffectively deployed within their organisation (e.g. matching is limited to certain business areas, at set intervals, and/or uses untested data matching rules). For fraud data sharing to be effective, it should be deployed across all business areas, at multiple points of the customer or client life cycle, and be utilised in real-time. Furthermore, well-structured data and tested, effective and in-built data matching rules are required to deliver legal and effective real-time data matching, which will minimise false positives and avoid inadvertently filtering out useful matches. It is this full and effective deployment of data matching that has saved over £1 billion for participating Cifas members in each of the last 5 years.

3.5.4 How can this be delivered by Government?

a. Government should not boil the ocean in seeking to deliver an uplift in benefits from increased fraud data sharing. Delivering a new common and secure platform for fraud data sharing would require substantial investment in time, resource and funds which it need not undertake.

b. Thankfully, Government need not build such platforms from scratch. Instead, it should utilise existing solutions which are already in use both by government and the private sector, and which are delivering quantifiable £/p benefits. Many of these solutions do not simply provide a data sharing platform, but also in-built analytics, training, and intelligence products.

c. Government should look to scale these solutions and expand its pilot activity within the framework discussed earlier – working to understand which solutions work where, how they can be best applied and rolled-out, learning where different agencies and departments

have challenges and capabilities and allocating pilot work appropriately, and understanding where economies can be achieved through scale across HMG.

d. The capability and resource to roll out such pilots needs to be built up across HMG – from pilot management, to fraud team and analytical capability. However, this relatively small investment in resource is dwarfed by the scale of the prize on offer. Indeed, there is a responsibility to the public purse to pursue this activity and ensure that maximum fraud loss prevention value is delivered.

3.6 Equifax – The power of Open Banking to improve services and tackle fraud

3.6.1 The power of Open Banking to improve services and tackle fraud

If data and technology are now the most powerful tools to transform public services, then the UK is enviably well placed to take full advantage.

People in the UK trust digital services more than in other OECD countries[1]. Financial technology attracts more investment in the UK than in the next nine most successful European economies combined; globally only the US and China do better[2]. At the same time, the Government is staking out ethical guardrails for the digital economy through the new Centre for Data Ethics and Innovation while leading the world in opening up access to data for the public good[3].

These strong foundations mean people in the UK are often the first to get a better service as a result of sharing data in new ways. A perfect example can be found in that most British of ambitions: buying a home. Dan, who works for Equifax in London, remembers that he had to wait six weeks to get his first mortgage. The biggest delay was caused by slow data sharing. The only way Dan could prove his identity, that he could afford the loan and was unlikely to launder the money was to send his lender six months of bank statements in the post.

When Dan next moves home he expects to find the process much improved. M&S Bank now accepts statements online[4], no matter who the applicant banks with, and other lenders will follow. Not only is it more secure – no chance of statements getting lost in the post - but M&S customers find out much more quickly if they can buy their new home.

What makes the M&S approach possible is Open Banking, a combination of new regulations and technology that lets consumers instantly share data about their bank account, and how they use it, with other organisations. Few countries have been able to turn the potential of Open Banking in to everyday services people embrace as quickly as the UK, thanks to that combination of trust, investment and a strategic approach from government.

Another way people are using Open Banking is to prove they are who they say they are. It lets you use your bank to vouch for your identity – your highly secure online bank log in unlocks services with other organisations.

3.6.2 Fast identity verification lets organisations improve services and reduce fraud by moving data

Fears about rising identity theft prevent organisations from sharing data that could otherwise reduce fraud or improve the services people get. The Centre for Counter Fraud Studies estimates that identity fraud costs UK adults £5.4bn a year[5]. Cifas, which maintains a database of identity fraud, recorded 175,000 cases in 2017, a 125% increase compared to 10 years ago[6].

The potential of Open Banking to overcome this barrier by allowing people to prove they are who they say they are is only just being explored. Scandinavia, where people have used a similar bank-backed digital identity for many years, points to what is possible in the UK.

Erika, a doctor in Oslo, uses her bank account to prove her identity several times a day. To buy things online, check her student loan or split the bill at lunch, she uses a service called BankID. Each time Erika has to prove who she is, BankID sends her a code on her phone that she unlocks with her thumbprint and enters in to an app. BankID is so widely accepted that Erika has not been

to an office to use a government service or bank for years. In the health service, her patients can use the same system to get information about their treatment, medicine and upcoming appointments.

In short, by giving people a way to quickly and easily prove their identity and then move data about themselves between organisations, Open Banking can improve services and reduce fraud well beyond financial services.

For example, vulnerable people are more likely to be in debt, have less financial stability and find it harder to explain their changing circumstances to the organisations chasing the money they owe. With Open Banking, someone in problem debt could share their financial information with a trusted third party, like a debt charity, in real time. If they had a sudden drop in income or a spike in essential spending, then the charity could alert debt collectors in the public and private sector to take less money that month.

Water companies could use the same type of solution to automatically move someone on and off social tariffs as their income changes. The public sector could use it to verify people's ongoing eligibility for support and make sure they get the right amount of money. It could also make it easier for citizens to claim the welfare support they are entitled to as their financial or personal circumstances change, either by sharing their data directly with the government or with a trusted third party, like a housing association or charity.

3.6.3 Empowering consumers to move public data so they get a better deal

The Competition and Markets Authority has suggested applying the principles of Open Banking to other markets so vulnerable consumers, or their time-pressed carers, can move their data to get a better deal[7].

A lot of the data consumers can use to get a better price or service is held by the public sector, and it is not just vulnerable people who benefit when they get more control of it. In some parts of the country, social housing tenants already ask their local authority to verify that they pay their rent on time as a way to improve their credit score.

The secure identity checks and technology that underpin Open Banking could allow people to move much more of the data public bodies hold about them.

If they were empowered to do so, someone could choose to share data about their student loan payments or Universal Credit income to access more affordable credit. If some people consented to use an Open Banking type system to verify their identity or to share data about their circumstances, then the organisations charged with preventing fraud could focus their resources on higher risk cases, saving more money for taxpayers.

3.6.4 Leading global innovation in technology and regulation, the opportunity in the UK is huge

Such prioritisation would be in step with global innovations in identity fraud prevention that use advanced technology and analytics to assess the risk a potential fraudster poses, then deploy different checks in response. Someone logging in to make a payment that is assessed as low risk might only have to use an app on their phone, whereas a log in or transaction that arouses more suspicion might trigger a facial recognition test and questions about personal information that only the true account holder could answer.

One such service is OnlyID, developed by Equifax and FIS in the US. It combines advanced analytics, real time data and evidence from 800 million consumer and banking records to spot and respond to high and low risk cases of fraud. OnlyID becomes more effective at preventing fraud the more data it draws on, and its users do not need to remember any passwords.

To understand what is possible with this new technology, innovators need somewhere to develop their ideas without putting citizens and their data at risk. The Financial Conduct Authority created FCA Innovate, a sandbox where developers can experiment with new products and services, and the regulator can learn how to regulate them. Regulators around the world have copied that approach in finance and the Information Commissioner's Office is now developing a sandbox to support innovative uses of personal data.

To promote an Open Banking approach to counter fraud, the Government could initiate a sandbox of its own. Not only would the sandbox set the rules for safe experimentation, but it could include datasets, tools and platforms for developers to use in their designs. Building on the success of the Rent Recognition Challenge, funding for new challenges linked to the sandbox could stimulate innovation to solve the most pressing problems.

M&S and others are already using Open Banking to make a difference for their customers. It will soon feel old fashioned that the only way Dan could move his data between banks was to mail hard copies of it from one to the other. The potential for Open Banking to tackle identity fraud and become a model for moving data between organisations in other sectors means its impact could extend beyond financial services however. At the forefront of worldwide Open Banking innovation and with such strong foundations upon which to build digital services and innovative regulation, the UK is exceptionally well placed to lead the way in discovering these other benefits too.

3.6.5 About Equifax

Equifax is a global data, analytics and technology company. Headquartered in Atlanta, Georgia, Equifax operates in 24 countries and employs approximately 11,000 people worldwide. In the UK, Equifax Ltd is authorised and regulated by the Financial Conduct Authority and is one of the three main credit reference agencies. Equifax is a Living Wage Employer and a signatory to both the Armed Forces Covenant and HM Treasury's Women in Finance Charter.

1. OECD (2019) Going digital toolkit.
2. Innovate Finance (2019) 2018 FinTech VC Investment Landscape Report
3. World Wide Web Foundation (2018) Open Data Barometer: leaders edition
4. Finextra (2019) M&S Bank enables faster mortgage applications with open banking.
5. Centre for Counter Fraud Studies (2016) Annual Fraud Indicator 2016.
6. Cifas (2018) The Fraudscape.
7. CMA (2019) Consumer vulnerability: challenges and potential solutions.

Synectics Solutions – Collaboration & Data Sharing

Collaboration & Data Sharing

Collaboration is the only way organisations seeking to counter fraud and financial crime can compete on a level playing field with the organised criminals

> Fraud is now the most common crime in the UK, with fraudsters working together to operate successfully. Could collaboration enable organisations to fight back and gain the upper hand in the fight against fraud?

According to the Office of National Statistics there were 5.8million fraud and computer misuse crimes in 2017, making them the most common crimes in the UK. Sophisticated technology is enabling criminals to steal and sell data globally on a scale never seen before, and to commit fraud in high volumes.

Research has shown that criminals often collaborate via restricted user groups on the public Internet as well as accessing 'dark web' closed user groups - sharing fraud methods, identifying weaknesses in target businesses, and developing new ways to commit their crimes.

This presents a huge challenge for law enforcement, government organisations and private sector industries, such as financial services, as they seek to prevent and detect fraud and other types of financial crime. There is also an additional challenge to meet consumer demands for faster decision making online when applications for credit or access to welfare benefits and services are concerned, which adds further pressure on organisations vetting and checking systems.

Synectics Solutions is the leading consortium data and data collaboration services provider in the UK, with over 27 years' experience creating, hosting and managing a variety of large-scale data collaboration programs that have helped to prevent billions of pounds being lost to fraud and financial crime.

With a truly unique body of expertise across sectors such as; UK Government, Banking, Insurance and telecommunications to draw from, we are well positioned to navigate the obstacles to enable enterprise and industry wide successful collaboration programmes. This ensures our clients' can easily and cost effectively pick their way through the regulation, legality, technology and other process challenges to successfully get their data collection and collaboration solutions off the ground.

Could sector-wide collaboration be the solution? In depth research indicates that it is an essential weapon in the fight against fraud.

As technology continues to evolve, we all become much more dependent on faceless, remote internet based processes to access the vital financial and government services that are essential to daily life.

Therefore, checking and verifying the true identify of individuals continues to be an increasingly important battle. Increasingly the diversification of an individual's data footprint will continue to grow. Most fraudsters are opportunistic and this is often happening through changes in personal circumstance driven by life events. Being able to map and record this information will provide intelligence that can be used to prevent fraud then regularly detect fraud.

Our research also showed that there is huge improvement in accurate fraud and financial crime detection where data is organised in a way that it can be cleansed, verified, orchestrated, shared and analysed with minimal friction and across organisations.

Fraudsters operate wherever there is a route to money and a potential victim. They share tips with each other and tell each other when a fraud works well and who are the easiest targets. They're not short of money to invest in research and technology and of course they operate outside of any laws or regulations.

Therefore, to mitigate this growing risk organisations must remove the silos that exist between themselves and the insular thinking that stifles the fight against fraud. As we continue to find newer and better ways to detect fraud, these strategies must be shared - ensuring the foundations of collaboration are in place to fully benefit from improvements made by organisations and fraud detection specialists.

This improvement needs to be done through data sharing across multiple industry sectors as well as between public/government and private sectors.

Why? Because that's one of the only ways in which we can successfully stay ahead of the ever-evolving strategies that are shared amongst financial criminals.

Synectics have understood that there are four main areas of focus that should be embarked upon with some urgency in this regard, before societies fall further behind fraudsters and financial criminals.

1. Expanded data collection programmes:
    - See step one below
    - See step two below
2. Strengthened capability and widened scope of supporting legislation
3. Investment and greater use of new technology
4. Increased access across organisations in both public and private sectors

1. Expanded data collection programmes

Step One:

An individual's data footprint comprises both structured and unstructured data. Structured data is more common and traditionally comes in easily readable and extractable text form. Synectics believe that robust new data collection programmes should be initiated, expanding across both public and private organisations to produce a more accurate reflection of an individual's true identity.

There is also a need to encourage all government departments to share data they hold, and work collaboratively to share intelligence and insight for the greater good.

This does not mean spying on society, but by using clearly visible fair processing notifications we can utilise the full potential of the current GDPR regulation. Key datasets would include but not limited to;

- DVLA
- Land Registry
- Investment organisations
- Births, Divorce & Marriages
- DWP
- Landlord information
- Credit Referencing
- DBS
- GP Registrations
- Homes England

Step Two:

Unstructured data should also feature in the data collection programme allowing it to be mined in an attempt to enhance and uncover new reference points relating to an individual's identify and behaviour. This should include the capture and analysis of multimedia such as photos, videos, audio and social media interactions.

2. Strengthened capability and widened scope of supporting legislation

Alongside this, Synectics think that government needs to expand the existing mandates it holds, as well as deliver new legislation to effectively allow data captured to be analysed, manipulated and shared. The introduction of the Digital Economy Act has enabled and encouraged and prompted government organisations to share data for the common good. Through various proof of concepts this has realised the value in data sharing, which can deliver tangible benefits to both financial and social to society. This needs to be expanded out, encouraging other Central Government Departments to do the same e.g. DVLA, Home Office and Land Registry.

3. Investment and greater use of new technology

Technology needs to be harnessed to deliver this programme in its entirety. Data has a set of variables that impacts its effectiveness:

Recency & Frequency; how old is the data? how often is the data collected?

Its appearance/origin - what does it comprise of etc?

Embracing analytics can reveal patterns and behaviours to help prevent fraud, advanced network analytics with real-time screening is the key to early fraud detection and prevention.

All of this needs to be presented in a format that is easily accessible and easy to use as not every organisation has staff, who are fully trained fraud investigators. Connections, inconsistencies and errors need to be made clearly visible so remedial actions can be taken swiftly and efficiently.

£44 billion

The Financial Cost of Fraud 2018 report estimates that the UK economy could be boosted by £44 billion annually if organisations step up efforts to tackle fraud and error

4. Increased access, data sharing and participation across organisations in both public and private sectors

Improved performance in fraud detection, the collection of insight, the development of new capabilities and better exposure will only be achieved if organisations expand and work with a wide host of other entities across public and private sector organisations.

This also involves working with organisations who provide outsourced support including: human resource management, asset management, supply chain management, accounting, customer support and service, computer software systems.

The collection and release of this data into various vetting and customer management systems will provide choice and value to end users to facilitate increased usage of the data as it feeds into existing systems already in use.

A data sharing and collection programme of this magnitude will fundamentally change a lot of things in the UK for the better if users and contributors are compelled to investigate and report usage outcomes.

Changing the mind-set of both the public sector and encouraging private sector organisations to share insight could be easily achieved through the exploration of new commercial performance related revenue sharing models and a series of re-education programmes.

Fraud poses a very real threat to every area of our lives and with every case there is a victim. The common view that some fraud is a victimless crime is far from the truth. With the main increases in fraud being made by falsification within applications processes, and areas such as identity fraud and false insurance claims, accessibility to data in real time needs to be a priority.

Continued development and increased use of automated data transfer methods such as SFTP and API's to ensure data is collected

quickly and efficiently will lead to real time decisioning, monitoring and alerting, which intern will help in our fight against fraud.

Looking at key life stage data, family connections, links with social media interactions, purchasing history and various other key registration data would greatly assist in providing information to identify such fraud & error.

This data however, needs to be harvested/ updated on a regular basis i.e. every 2-3 weeks as a minimum.

Key areas of development

Area of Development	Definition
Better information	Data that is accurate and timely, specific and organised for a purpose, presented within a context that gives it meaning and relevance, and can lead to an increase in understanding and decrease in uncertainty. Information is valuable because it can affect behaviour.
Access & Enablers	The means an opportunity to approach, enter, retrieve or obtain information, something or someone that makes it possible for a particular thing to happen or be done.
New Technology	Evaluation and implementation of new technologies that are currently developing or will be developed over the next five to ten years, and which will improve the way systems, products are produced.
Increased Capability	Invest in the capability you have already built. The ability to do something different, better, faster, more economically or more often.
New Partnerships & Channels	Is a third-party organisation or individual that works together to provide access to new technology and capability or markets and sells products, services or technologies to a defined customer base of new or existing customers

Areas of considerable impact

1. Housing Tenancy and Household Composition Insight

The greatest increases over the past 12 months occurred in real estate, rental and leasing fraud – which saw the total value shoot up to £276.5 million from £1.08 million

Source; Consultancy.uk

Social housing letting costs

Source data: FFR 2018

Unlawful subletting of a social housing property, whether owned by a Local Authority or Private Landlord is a criminal offence under the Prevention of Social Housing Fraud Act 2013.

Private registered providers manage around 2.8 million home and local authorities still manage around 3.1million homes.

Housing or Tenancy fraud is thought to cost housing associations and local authorities in the UK around £955 million a year. It's estimated that around 1% of social housing properties are fraudulently let.

Overpayments on Housing Benefit were recorded at a rate of 6.7% equivalent to £22.3bn. A focus on this key area would reap significant benefits in fraudulent housing benefit claims.

Actively working with social housing organisations and federation groups to either mandate or offer free data submission to allow the government to create a comprehensive picture of the housing landscape will help tackle this problem. This will also support the payment of Housing Benefit and provide a detailed picture of individuals whereabouts to support household composition and associated benefits or services being claimed.

The supply and running costs of 59,000 homes to housing provider s @ £24,000 per year leads to over £14.16m of lost revenue; this does not take into account wasted time and resource investigating fraud and managing housing assets.

2. Identify Verification – Fraud Prevention

As we embrace technology and mobility, face to face interaction with individuals will inevitably decline in the digital world, so knowing your customer becomes more difficult.

Primarily it's about improving the efficiency and reliability of verification, so if we request specific documentation to be presented, then we must move quickly using machine-assisted verification.

This goes beyond verifying the documentation being presented but looking for unique reference data/points to verify the true identify of an individual.

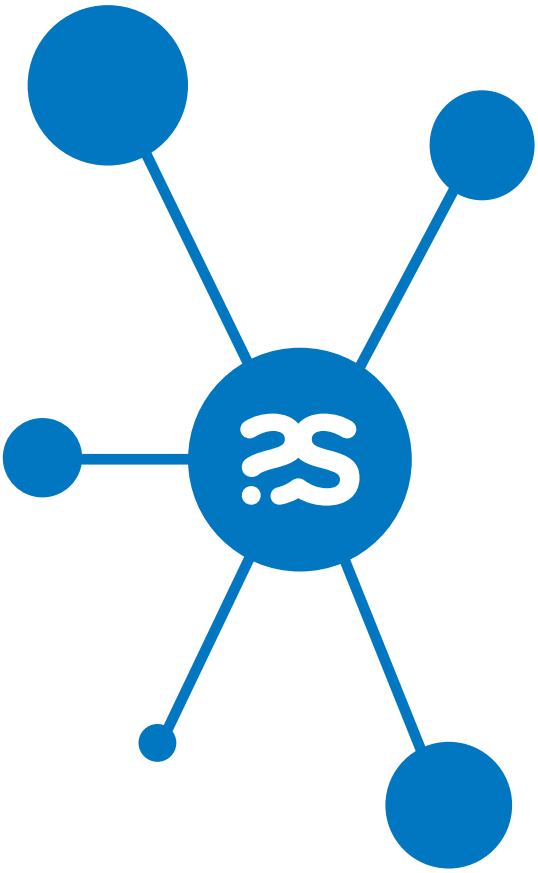
This affects so many organisations and would deliver significant benefits for all but could be a major game changer for the NHS.

Outside public sector the opportunities are well defined with over 9 million credit reference or fraud checks taking place every week within the UK. Fraudsters are more likely to use stolen genuine identities rather than fictitious identities as they are more likely to pass verification checks. This widespread use of genuine identity details makes identity fraud increasingly difficult to spot from genuine applications. Hence this is why we feel the use of the NFI dataset within the private sector is a missing piece of the jigsaw to provide organisations a positive verification as well as a negative one.

Way Forward:

Implementation would need to be phased, building on the investment already made.

1. Expand the capability of the NFI web portal as the Cabinet Office has already made significant investment here and this could be easily be expanded and shared more widely.
2. Data enrichment from new public and private data sources to expand and enhance current data matching (including unstructured data)
3. Greater introduction of predictive analytics, risk profiling and machine learning
4. Set basic fraud prevention best practice standards and benchmarks, supporting the introduction of verification processes across the life cycle of citizens, encouraging basic due diligence to be incorporated, utilising both public and private sector data



3.7 TransUnion – Developing a data mindset – opportunities for improving the UK's government data and analytics capability

3.7.1 Context and background

A feature of both public and private sector organisations today is their reliance on quality data and the ability to create actionable insights from them. As one of the UK's leading credit reference agencies, TransUnion (formerly Callcredit), has at its heart a keen focus on the power that data and collaboration can bring as Satty Saha, CEO of TransUnion in the UK explains:

"We're in the middle of an explosion of new data sources, led by the digital revolution. This together with exciting new analytical techniques and computer power enables us to do more good with data. Not only can we further reduce fraud to bring society benefits, but we can be part of the creation of a fairer and more transparent ecosystem to ensure that both the wider economy and consumers can benefit from the enhanced level of data and insight we have available today."

As a global risk and information solutions provider, with a presence in over 30 countries, TransUnion has worked with governments around the globe on initiatives ranging from healthcare to financial inclusion, bringing its expertise in data and analytics and its deep-seated philosophy of 'Information for Good' to the public sector, to support the creation of enhanced public services.

With an innovation-focused data mindset – working within the frameworks laid out to protect data privacy and security of consumer data – government and private sector collaboration in technology development can help ensure that public services can take advantage of the latest thinking and technology and utilise lessons learned in the private sector to deliver a public service that puts the consumer first, overcomes challenges to reduce fraud, and creates a responsive, responsible infrastructure for a strong nation.

3.7.2 Data mindset – what it means and how to use it

The shift away from purely qualitative evidence for creating services and policy is a positive step. Not only that, but the introduction of data-dependent services that can react in near real-time to changing individual or organisational circumstances is crucial to a 21st century service provider – public or private sector.

The professionalisation of data science, the development of a data mindset, and the acceptance of the benefit it brings is no longer a niche interest. The UK Government (HMG) has made clear steps towards this goal, which we welcome. TransUnion sits on the data sharing and data analytics advisory panel and we have provided support and insight on the creation of good practice guidance to implementing data analytics to counter fraud in government. We look towards initiatives such as the Cabinet Office's development of the data-led counter fraud strategy and profession as key reference points to support this.

By this term – data mindset – we mean an organisational, all levels, recognition of the value of data, along with the drive to use it and the policies and structure in place to make sure results deliver on a strategic objective. It means a focus on innovation, educating and upskilling, and the development of use cases (such as countering fraud) that have long been desired but previously challenging to execute. It also means compliance with all applicable laws and regulations, robust information security practices and, as TransUnion sees it, being a responsible custodian of data.

Introducing a data mindset, and investing in the tools and processes to enable it to bear fruit, when done responsibly can be used not solely to displace human capital, but to drive more effective use of that precious resource. Robotics and automation, which are now reasonably widespread in the private sector to replace manual intervention are only effectively deployed based on better data and enriched insights. Analytics supports that process enrichment.

TransUnion has worked alone and in partnerships to develop products, in both the public and private sector, based on smart data techniques like machine learning. A data mindset, perhaps more than the availability of the technology, is the real catalyst for these projects and we are greatly encouraged to see its continuing evolution among our public-sector counterparts.

3.7.3 Quality raw materials lead to quality results

Developing a mature data-focused organisation means not only ensuring the team's skills and the technological infrastructure is in place, but that there is serious work being done on implementing data standards and data dictionaries to clarify and align the meaning of data. Sourcing top quality, clean data and using it for positive purposes is of key concern. Key focal points in this discussion are the use of open source and shared data sets, and the mitigation of the risks that come from the highly regulated practice of sharing data.

3.7.4 Sharing

The National Data Strategy is designed to unlock the power of data in the UK economy and government, with the potential to create a truly world-leading data ethics and strategy framework.

HMG has shown progress and leadership in data sharing through its enactment of the Digital Economy Act 2017 as a mechanism to safely share data. The Act is closely aligned to the objectives of the 2002 Cabinet Office report on privacy and data sharing which set out, "to improve public services through better use of data while safeguarding citizens' privacy." In addition, HMG encourages departments to "release operational data in electronic open formats that encourage reuse and develop new applications" through its Open Data Agenda.

In TransUnion's view, the government's data sharing practices show great potential, though have not yet gathered critical momentum to deliver on what it needs to be truly classed as holistically effective. However, numerous data exchange projects between public and private can be used as evidence for the success of collaboration. Projects like the one TransUnion participated in to introduce risk based verification within housing benefit administered by local authorities – which delivered on its aim of improving the time taken to process the majority of low-risk claims whilst reducing overall error and fraud in the administration of housing and council tax benefit, as well as improving customer journeys for claimants – can be seen as verification of the data-led approach in public services showing serious results, as well as other projects where fraud prevention organisations have led the charge in sharing data across sectors.

With the ground laid for collaboration, focus will soon turn to more ambitious projects to create value from disparate data. Private sector organisations such as ours can provide a valuable service in interpreting the data we have and the value/proof points it helps public sector organisations create. In fraud alone – specifically to fight money laundering or adhere to Joint Money Laundering Steering Group guidance – using collaboration and shared data to create machine learning (ML) models to predict fraud through enhanced analytics can offer the public sector a leap forward in capability.

Knowledge-sharing across sectors can bring clear two-way benefits, and will assist in the development of the government's Digital First servicing of citizens, by taking learnings from the private sector where many organisations are digital-only.

3.7.5 Risks

Private sector companies can provide insight on collaborative data assignments to government bodies in areas of compliance, due to their experience in aligning projects using shared resources to regulations and standards, and adoption of changes to that landscape – GDPR being a prime example. For example, TransUnion is an FCA-regulated business and we operate under a range of legislation including the GDPR, the Data Protection Act 2018 and the Consumer Credit Act 1974, as well as the FCA's rules. Collaborating with counterparts in the public sector who bring deep expertise in navigating and executing nation-level projects ensures a full spectrum of skills and capabilities can be brought to bear. Organisations such as TransUnion can use their experience to augment public sector organisations' existing skills to ensure the smooth, effective delivery of public sector projects – as well as to promote innovation at an arm's length to public data bodies, enabling government to benefit by proxy.

It is by no means a one-way street – private sector organisations also have a lot to learn from the public sector. TransUnion commends the government's leadership on data regulation and guidance on best practice use – particularly it's proactivity in creating the Data Ethics Framework in 2018, active membership in the EU's eIDAS knowledge and learning programme, as well as the recent appointment of the first national data guardian for health and social care. Projects set up under structured guidance have already shown promise. We see that creating a forum within a defined CUG (closed user group with defined sharing purposes) can lead to great benefits – a key reference point is the Cabinet Office-led National Fraud Initiative, an example of where specified anti-fraud organisations could have a role to play in supporting public sector on shared data projects.

3.7.6 In the right mindset – now put it to work

We would like to close on actionable ways to enhance data analytical capability extracting greater value from the data that can be accessed. Across the broad spectrum of public service, there are potential avenues for advancement – our particular concern is helping improve fraud analysis and prevention. TransUnion research with private sector fraud prevention leaders carried out in May 2018 shows us that 90% of them pinpointed implementing fraud prevention technology as a priority, up from 76% the previous year.

Artificial intelligence (45%), machine learning (37%) and biometric screening techniques (37%) are being targeted as the top fraud prevention solutions over the next three years, whilst 90% said they would introduce a form of ID verification by June 2019. Noting that data techniques can often be used to evolve or build existing capabilities, as well as develop new ones, TransUnion's Managing Director of Fraud & ID John Cannon points out:

"These figures reaffirm the importance of the balance between more traditional techniques and emerging tools. Whilst organisations – private or public – need to keep up with the latest developments, such as the forensic profiling of device, email and mobile attributes, these should serve to enhance existing verification techniques."

One way of the government taking the lessons of the private sector, in this area alone, is the creation of a fraud hub, or sandbox. A sandbox is a technical environment where ideas and solutions are tested before being trialled publicly – a safe space so that HMG can quickly test and learn with data and analytics from disparate sources in a compliant way. Syndicated data services and open source platforms already exist, and are utilised by TransUnion in multiple geographies, so with combined public and private skillsets the toolkit is there to deliver it in a cost-efficient manner. This could allow for safe experimentation and testing to create machine learning models to predict fraud through enhanced analytics.

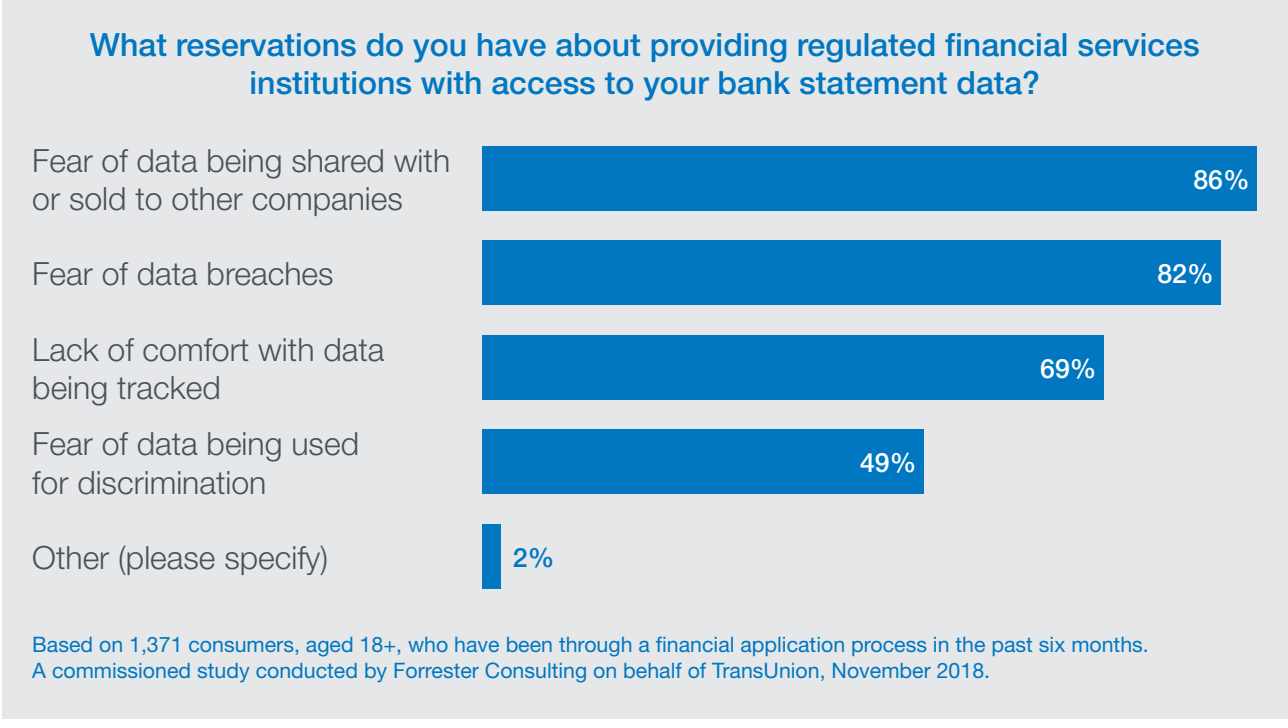
3.7.7 Future focus

While the future of capability in creating a data mindset culture and delivering data-driven services is not in doubt, and machine learning specialists are in particular demand, the future of data in public and private sector will be dominated by the response to key human concerns. Chief among these are data privacy, ethical and security considerations, bias in AI-derived decisions, future legislation and political changes and consumer education.

One area where these factors come into sharp focus is in the UK's new Open Banking initiative, which aims to provide consumers with a trusted route to realise the power of their own financial data. TransUnion launched its own end-to-end Open Banking service earlier this year, specifically designed to assess income and expenditure, affordability and creditworthiness and, alongside this, researched attitudes amongst UK citizens and the financial services sector toward the implementation of this new technology.

TransUnion's white paper, 'The Evolution of Open Banking' found that the main barriers to consumer adoption are fear of data being shared or sold to other companies (86%) and fear of data breaches (82%). Such fears over data use among consumers could mean restrictions on data projects in public sector – a risk that can be mitigated with effective public education, training and upskilling.

Fig.6 from The Evolution of Open Banking: Evolution, Benefits and Consent.



Consumers are the most important stakeholder in any data-led process. No matter how developed the technical capability, how secure the data transit, analysis or storage is, how dedicated the team – without a focus on delivering a true, honest and transparent benefit that empowers consumers then projects will fail.

HMG is dedicated to finding new ways to use data to fight fraud. This thought paper demonstrates TransUnion is similarly focused on this and we look forward to the opportunity for ongoing future collaboration.

Contribution 4. Academia

4.1 Dr. Georgios Samakovitis, School of Computing & Mathematical Sciences, University of Greenwich

4.1.1 Proposal Brief – Data Sharing

This brief proposes core areas that, we believe, should form thematic entities in the Cabinet Office Thought Paper on the benefits of enhanced data sharing capabilities to UK businesses, the wider community and civil society. This comes on the back of the Office's Counter Fraud initiatives wherein the critical value of information sharing is highlighted.

We propose a thematic taxonomy that serves as a suitable conduit of priorities to be identified through consultation with industry, government and academia. The taxonomy is aimed to work as a scaffold that will also accommodate any additional themes coming out of Parliamentary Debate on the back of the Thought Paper.

The taxonomy is developed in light of two pertinent observations:

a. New and emerging market and technological infrastructure[13], coupled with innovation in the space of identity management & verification, suggest an upgraded role for the user – citizen as data owner in the new data exchange ecosystems: therefore, the possible future role of the user of new data-centric technologies should be accounted for, as the responsible and accountable custodian of their own personal data; in the same vein, ways that such data are accessed and ringfenced should be explored;

b. Stemming from the above, a need is pronounced to further embed the subjects of data awareness and digital identity as integral parts of the curriculum in UK Secondary Education; that should be stressed as a step to future-proofing society from the challenges to come in the digital economy (as outlined according to the HMG Digital Economy Act 2017);

The thematic taxonomy is grounded on:

- The novel capabilities and affordances of new technologies, particularly those classified under the umbrella of Artificial Intelligence (AI);
- The detriment areas, as pronounced by government, businesses[14], consumer groups and representative bodies of the civil society;
- The government priorities in technology and innovation policy, market regulation and consumer protection;

13 Numerous developments materialsed in the past 4-5 years, particularly in the area of Payments and identity management, which surface new emerging roles for the user-citizen: the establishment of Open Banking standards, advances in API (Application Programming Interface) technology and capabilities made possible through innovations such as Distributed Autonomous Organisations (e.g. blockchain) have introduced a far more granular network of services and market actors than before. It is projected that the same innovations allow the user-citizen to make more direct and active use of their personal data, though selective sharing, remunerated through micro-payments.

14 A thorough analysis of detriment areas concerning Data Sharing (albeit concentrating in the field of Payments only) was carried out in early 2016 by the Payments Strategy Forum (UKPSF; https://www.psr.org.uk/psr-focus/payments-strategy-forum)

Two themes are proposed as core and a third as an overlay. These are discussed in more detail in the following sections

4.1.2 Theme A: Towards frameworks for AI Ethics - Uses in persistent[15] & pervasive[16] identity and related risks.

Mainly driven by the exponential growth in computational processing power, the respective drop in data storage costs, the pervasive use of personal user sensors (primarily through smartphones) and cloud computing, the application scope of Artificial Intelligence has experienced a similarly explosive growth. Critical for both the efficiency of intelligent decision-support, and the regulation around beneficial use of AI is the discussion on how information (especially data related to personal identification but also verification of ownership and status of non-human entities, such as physical and intellectual property) is acquired, stored and updated, as well as how quality of that data is preserved.

Most important concepts to be explored are those of pervasive and persistent identity, especially in view of the risks (primarily technical and ethical) associated with both the establishment and the usage of identity.

Government plays a critical role in this development as both a user and policy maker. From a user perspective, a great number of government application areas are being presently rehearsed. Counter-fraud is merely one of the areas where AI can deliver sizeable performance and cost-related improvements, extending to use cases in benefits misappropriation, government grants allocation, and money laundering to support illicit activity (threat finance).

From a policy perspective, it is proposed that, on the back of its recent Industrial Strategy, HMG addresses two areas where this should be assessed:

a. The extent to which capabilities or affordances are useful in practice - in the sense that what can be achieved is not necessarily desirable - and the role of regulators in determining this;

b. The extent of delegation of decision to AI. Risks include the hard-wiring of human assumptions into machine intelligence and the often-false assumption that faster intelligence will deliver better intelligence; This conversation underlines the need for assessing:

   - The extent to which the user should trust AI agency in decisions that affect them;
   - The extent to which Government should trust AI agency in areas that may affect policy, directly or indirectly;
   - The extent to which the balance between explainability and accuracy of AI techniques will determine trust and, subsequently, adoption of AI.

Further analysis and a more detailed proposal can be provided by the author of this report as and when this would be desirable.

4.1.3 Theme B: Data Quality and the limits of Analytics capabilities

On the back of the wider conversation around AI Ethics and the central role of identity, the second proposed theme is that of Data Quality and data usage. As outlined under Theme (A) above, the quality of information used to train and test the efficacy of AI agents is a critical parameter for the effectiveness of AI-based decision-support.

15 Persistent Identity: “a fixed set of identifiers...associated with a person so that he/she can be recognized or distinguished by others and by society in general” Gilbert et al (2014)

16 The term Pervasive Identity refers to the capability of the entity carrying it to be uniquely identified across different platforms, applications or systems.

Ensuring Data Quality comes with a series of challenges (again, both technical and ethical) including, but not limited to, the following:

a. The means and processes through which the sources of data will be vetted, (bearing in mind that, among legitimate data sources, no single source contains all correct information and that not all information available is updated);

b. The jurisdictions and regulations governing different data sources;

c. The means and processes through which decisions can or should be made on what will ultimately constitute the official version of the data (a.k.a. “single version of the truth” (SVOT))

d. The moral and ethical limitations of how that data will be used equally by the Government, business, or the citizens themselves.

Especially the latter challenge (outlined as item (d) above) raises the issue of limitations of Analytics as a class of decision tools. The technical capability for delivering usable (often in near-real time) insights on data has been highlighted in numerous commercial applications, and has also been demonstrated in recent Counter Fraud Analytics projects of the Cabinet Office. Again, it is proposed that it should be the imperative of Government to ensure that such capabilities:

a. Are suitably situated into wider decision-support frameworks, as opposed to becoming adopted as automated decision-making tools;

b. Are designed to make use of data in context (rather than solely deriving context from data);

c. Are used for applications which are within the broader Ethical Codes.

4.1.4 Theme C: Distributed Autonomous Organisations (DAO) & Smart Contracts (Blockchain): applications in fraud, identity and beyond.

The third theme is proposed as an overlay to the aforementioned themes, in the sense that it recommends a class of technologies that may offer potentially strong technical implementation for (i) persistent and pervasive identity; (ii) the wider implementation of ethically robust AI agents; and (iii) securing data provenance and quality. Strong Use Cases for DAO and Smart Contracts include, but are not limited to, KYC and Onboarding, Fraud Detection and Anti-Money Laundering, IPR verification and automated royalties payments, property contracts, 'programmable money' (special-purpose money), land registry applications and more.

While there has been significant hype around Distributed Ledger technologies, evidence suggests that the underlying protocols and techniques do constitute solid vehicles for radical innovation as is also testified by the present investment in those technologies, estimated to reach $11.7bn by 2022.

This brief recommends the wider and deeper engagement of HMG into not only testing funding and promoting more solutions and systems for internal application, but also into nurturing the establishment of UK Centres of Excellence in Blockchain, Smart Contracts and DAO technologies. Broadly the high-level areas that we recommend are addressed include, but are not restricted to the following:

a. The identification and assessment of the risks of using and the risks of not using DAO technologies;

b. The requirements for a Knowledge Base in Government and Regulatory Bodies, as the disruptive nature of those technologies necessitate solid understanding of the capabilities and limitations that can be supported and regulated;

c. Exploring the opportunities to leverage the pervasive nature of DAO technologies across fields (adoption in Counter-Fraud may provide a strong starting use case, followed by applications in identity verification, onboarding, IPR assignment and beyond);

d. The affordances and capabilities of DAOs will have to be critically reviewed, especially in light of the aforementioned hype (which is historically endemic to all radical and disruptive innovations)

Finally, this brief recommends that the broader area of Cyber Security is an entire shell on its own right and can be embedded in the wider conversation as a layer in the infrastructure (technical and intellectual). As such, it may be best addressed in a separate Thought Paper, providing the opportunity to expand to subjects such as IoT, the connected self, and the role of educating end users to protect themselves, especially in view of consumerisation of technologies with enhanced capabilities.

Dr. Lucian Tipi PhD, MSc, BSc, SFHEA, CITP, CEng, Sheffield Business School at Sheffield Hallam University – Controlling Fraud, the framing issues

Sheffield Hallam University | Sheffield Business School

4.2.1 Abstract

This paper will discuss current challenges faced by governments and businesses in detecting and combating fraud alongside emerging technologies that may be used to reduce the volume and impact of fraud.

4.2.2 Challenges faced by governments and businesses

a. Absence of a unique person identifier

   The ID does not have to be a physical artefact – e.g. smart card. It can be an e-ID.

   Some of the benefits of a unique ID are:

   - One ID for all transactions
   - Streamlined information, less data sets
   - More efficient government transactions
   - Protection from fraud
   - It can be used in many ways

   Some of the drawbacks of a unique ID are:

   - Potential data breaches
   - Possible privacy rights violations
   - Difficulties in matching a real person with online persona
   - Use of biometrics and ethical and security issues associated with their use (e.g. IBM use of skin tone to identify individuals)

b. Multiple data sources and repositories within organisations

c. Data distributed across many organisations

d. Legacy systems and integration of digital supply chains (e.g. 50% of UK Councils still use unsupported software)

e. Maintaining data currency in a population where circumstances change often (employment status, residence and relationships)

f. The “Gig” economy shows very significant growth

g. Customer expectations of a 24/7 world, with immediate response to interaction

h. Shift to mobile platforms (smartphones) for large segments of population

i. Broad range of factors which demand very different ways of interaction (e.g. age and disability)

j. Lack of skilled coding and data analytics qualified staff

k. Lack of staff that can bridge the gap between technology and business

l. Security VS convenience skewed towards convenience due to a strong demand from online users for fast and easy access

m. Ethical issues around profiling of customers by using predictive algorithms

n. Organisations processes poorly understood, organisations still trying to fit businesses around technology (which is the wrong way around!)

o. Lack of true process automation (and auditing of automated processing)

p. Failure to take a goal driven holistic approach (optimising each part does not give an overall optimum!). Defining a robust goal is a challenge

4.2.3 Emerging technologies

a. Artificial Intelligence (AI)

- Touted as the next step change in computing and business
- Computing power only now reaching processing power and connectivity similar to the human brain
- Easily scalable
- Offers the potential of true human – machine integration (Industry 4.0)
- One of the biggest challenges around AI is that it is only as good as the data used to train it. Poor data results in poor AI engines
- True AI is still seen as some way off. "Consciousness" or "Self-awareness" are the ultimate goals
- Can automate human interaction processes on a large scale by using biometrics
- Can automate mechanistic/repetitive back office processes in a very cost-effective way (e.g. accounting, payroll)
- Challenges around auditable AI and decision making – bias can be built into algorithms very easily (e.g. Goole searches around political topics)
- Challenges around liabilities around AI – who is liable? (e.g. Tesco, ASDA introducing AI driven age verification)
- There is an enormous drive to develop AI by ALL major technology manufacturers and transformational production systems are already in place (e.g. healthcare and education)

a. Blockchain (BC)

- BC technology has built a very strong brand in a very short period of time
- Very prominent in virtual currencies, who are very popular yet very volatile
- Potential to completely disrupt traditional industry sectors (e.g. financial sector) – automated smart contracts and currency transactions
- Challenges around anonymity provided by BC and lack of regulation
- BC based payments technology is very easy, policy and regulation is hard
- A very large number of BC trials projects exist. However, worldwide only around 3% of these go into production. In the UK the figure is 22% - global leader
- The hype around BC tech is huge, yet most large technology manufacturers consider it to be immature. Having said that, they are all developing large BC projects
- Australia – trials on the use of BC for ID verification based on driving licenses concluded that technology is not yet good enough, can be done better with current technologies
- Microsoft – using BC to develop "online ID" mechanisms – huge global potential
- China – sees that potential value of BC exceeding the current combined value of Internet transactions and a good mechanism for regulation

4.2.4 Further work

It is envisaged that the exploration work around the areas introduced earlier will continue, with the UK Government, Business and Academia working together to ensure that progress is made to understand the nature of the challenges listed above and to ensure development of policy and process that will help to control fraud.

References for Section 4.2.2 Challenges faced by governments and businesses

a) Sources that support the evidence and discuss the risks of national ID schemes:

http://www.emeraldgrouppublishing.com/learning/management_thinking/articles/pdf/national_id.pdf

https://www.ft.com/content/2ec95b9a-4709-11e8-8c77-ff51caedcde6

https://www.gemalto.com/govt/identity/5-reasons-electronic-national-id-card

https://findbiometrics.com/4-national-id-programs-306150/

https://www.imoney.ph/articles/filsys-financial-implications

https://www.rediff.com/money/2009/jan/22guest-benefits-of-a-national-identity-system.htm

d) Source: The influential Computing magazine, 24/8/18

https://www.computing.co.uk/ctg/news/3061558/fifty-per-cent-of-councils-in-england-rely-on-unsupported-server-software

j) Source:

https://www.computing.co.uk/ctg/news/3029865/british-army-recruits-software-ag-to-improve-critical-information-sharing

https://www.computing.co.uk/ctg/news/3029867/newcastle-it-sector-salaries-boom-as-digital-skills-shortages-bite

k) Sources:

https://www.computing.co.uk/ctg/opinion/3030209/reorienting-your-workforce-in-the-age-of-ai

https://www.computing.co.uk/ctg/news/3030511/dcms-launches-search-for-new-data-expertise-after-pinching-gds-data-role

https://www.computing.co.uk/ctg/analysis/3062248/the-uk-needs-more-data-engineers-and-analysts-to-fuel-the-data-driven-economy-post-brexit

n) Sources:

https://www.computing.co.uk/ctg/interview/3030886/adopting-open-has-driven-change-in-the-uk-government

https://www.computing.co.uk/ctg/news/3069840/more-applications-more-complexity-what-is-driving-automation-adoption

o) Sources:

https://www.computing.co.uk/ctg/news/3062333/ten-fold-increase-in-security-breach-cases-since-gdpr-claim-lawyers

https://www.computing.co.uk/ctg/opinion/3063197/algorithms-in-the-justice-system-should-computers-decide-our-fate

p) Sources:

https://www.computing.co.uk/ctg/opinion/3035077/optimising-cloud-economics-to-future-proof-the-business

https://www.computing.co.uk/ctg/news/3035136/automation-will-increase-the-economic-wealth-gap

Feedback on the use of Data and Analytics to counter fraud threat

Return instructions on p.20

Your details (optional)

Your or company name:

Contact details (email):

	Please add your thoughts on each of the issues outlined in section 2 below:	We would appreciate any additional ideas you would like to contribute to this work:
	Q1. Should Government embed a Data Mindset, and how could it achieve this?	
	Q2. What should Government do to improve Data Quality, and should it seek to develop standardised data sets that can be consistently used and understood?	
	Q3. What more could be done to improve the tools staff have access to; as well as ensuring that they have relevant skills and capabilities to generate maximum value from using data to reduce fraud?	
	Q4. What should, and could Government do to improve access to counter fraud data in an economically viable way?	
	Q5. To what extent should Government seek to exploit the opportunities emerging technologies like AI could provide in countering fraud, and what frameworks could be put in place to ensure their usage is ethical?	
	**Other key challenges** Are there any other key challenges or observations you have from your own industry, or your knowledge of the public sector, and how would you recommend government approach them? We would also welcome any other ideas of feedback you would like to extend on the ideas discussed in this paper.	

Cabinet Office