National Audit Office

REPORT

Using data analytics to tackle fraud and error

Cross-government

SESSION 2024-25
9 JULY 2025
HC 988

The National Audit Office (NAO) scrutinises public spending for Parliament and is independent of government and the civil service. We help Parliament hold government to account and we use our insights to help people who manage and govern public bodies improve public services.

The Comptroller and Auditor General (C&AG), Gareth Davies, is an Officer of the House of Commons and leads the NAO. We audit the financial accounts of departments and other public bodies. We also examine and report on the value for money of how public money has been spent.

In 2024, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £5.3 billion. This represents around £53 for every pound of our net expenditure.

National Audit Office

Using data analytics to tackle fraud and error

Cross-government

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 7 July 2025

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Gareth Davies
Comptroller and Auditor General
National Audit Office

26 June 2025

HC 988 | £10.00

Value for money reports

Our value for money reports examine government expenditure in order to form a judgement on whether value for money has been achieved. We also make recommendations to public bodies on how to improve public services.

015415 07/25 NAO

Contents

Summary 4

Part One
How data analytics can tackle fraud and error 10

Part Two
The strategic challenges 22

Appendix One
Our audit approach 41

This report can be found on the National Audit Office website at www.nao.org.uk

If you need a version of this report in an alternative format for accessibility reasons, or any of the figures in a different format, contact the NAO at enquiries@nao.org.uk

The National Audit Office study team consisted of:

Marc Adams, Connie Woolen, Tabitha Beer, Liam Blanc and Christopher Barrett, under the direction of Joshua Reddaway.

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

020 7798 7400
www.nao.org.uk
@NAOorguk

Summary

1 Fraud and error in the public sector generally means an incorrect amount of money has been paid out or received by government, or government has made a transaction with an incorrect or ineligible party. We estimate that fraud and error cost the taxpayer between £55 billion and £81 billion in 2023-24.[1]

2 Data analytics are a vital tool to make sure the right amount of money goes to the right recipient, and to find potentially incorrect transactions. Such data analytics can range from basic tools that check a public body only paid a supplier once, to using emerging technology like artificial intelligence (AI) to identify risky transactions. Tackling fraud and error is a good test case for new technologies in data analytics such as AI. In theory, with good-quality linked data, these technologies can deliver more immediate returns on investment, tackling fraud and error without requiring the wider system or organisational reform that fuller digital transformation would require.

3 Public bodies are responsible for managing the risk of fraud and error in their organisation and delivery chains. To manage these risks, they should assess their vulnerability to such losses, evaluate the scale of the risk, and respond accordingly. Three cross-government functions have a role in supporting public bodies to tackle fraud and error using data analytics.

- **The Government Counter Fraud Function (GCFF):** The GCFF has a strategic objective to 'Harness data and technology more effectively.' It is led by the Public Sector Fraud Authority (PSFA), which works with public bodies to understand and reduce the impact of public sector fraud and error, provides counter-fraud and error data analytic services to local and central government, and encourages public bodies to make best use of data analytics to tackle fraud. PSFA reports to both Cabinet Office and HM Treasury.
- **The Government Digital and Data Function:** This is led by the Government Digital Service (GDS) which sets the digital strategy for government and maintains guidance and tools to support best practice. It sits in the Department for Science, Innovation & Technology (DSIT).
- **The Government Finance Function (GFF):** The GFF comprises the finance teams across public bodies, supporting them to manage money efficiently, including to make sure correct payments are made to and from the right people at the right time. Finance teams are supported by a central GFF team (based in HM Treasury), who set standards and good practice.

1 National Audit Office, *Good Practice Guide: Estimating and reporting fraud and error in annual reports and accounts*, February 2025.

4 This report examines how well placed government is to seize the opportunity offered by old and new data analytics technologies to tackle fraud and error. We look at what government is already doing and set out the challenges. The report sets out:

- case studies of how the private sector and government are already using data analytics to tackle fraud and error (Part One); and
- lessons from these case studies, and our discussions with those involved in implementing them, about the strategic challenges (Part Two). A summary of the challenges is shown on pages 8 to 9.

5 Our findings are based on the experience of those who have implemented data analytics tools. To build our understanding of the types of data analytics used to tackle fraud and error in government, and the associated strategic challenges, we wrote to the finance directors of government departments. We asked them to provide examples of data analytics used to tackle fraud and error, and we interviewed and held workshops with 24 counter-fraud teams involved in these projects. Appendix One sets out more information on our audit approach and evidence base.

Key findings

6 GDS believes government could save as much as £6 billion a year by using data analytics to help tackle fraud and waste. The use of data analytics to tackle fraud and error has the potential to save billions of pounds of taxpayer money. Counter-fraud experts, within and outside of government, consistently told us that data analytics needed to be a key part of any plan to reduce fraud and error. They highlighted how data analytics can help ensure public bodies pay the right amount to the right suppliers, receive the right amount of tax revenue and only pay grants or benefits to eligible recipients. GDS produced its estimate of £6 billion to give an indication of the potential savings. It based this on the savings the Department for Work & Pensions (DWP) has achieved in one example of data analytics and applied these savings to PSFA's estimate of the level of fraud and error across all of government. This implies that most of the savings would come from tax and benefits (who already use data analytics), but also that a significant amount would come from the rest of government. However, the estimate does not take into account the cost or effort needed to achieve the savings, or what needs to happen for such savings to be delivered, and as such should be read with caution (paragraphs 1.2 and 2.2, and Figure 1).

7 Data analytics are already a well-established tool for reducing the cost of fraud and error in the private sector. Many private sector organisations use different preventative data analytics tools simultaneously to protect their profits and customers from fraud and error losses. For example, banks told us they can stop potentially fraudulent payments being made if an account number and name do not match, if the account age or transaction history looks risky, or even if computer mouse movements suggest that an account has been hacked (paragraph 1.3 and case studies 1 to 6).

8 Some parts of government also already use data analytics to save money by preventing fraud and error, or by recovering money lost to fraud and error. DWP and HM Revenue & Customs (HMRC) have been using data analytics to tackle fraud and error for a long time. Much of their work involves data matching, networking, anomaly detection and predictive modelling to check that details provided match other data sources. Other public bodies are also piloting and experimenting with data analytics. Part One of our report sets out examples, including where public bodies flag risky supplier relationships using network analysis and data matching, identify duplicate payments and analyse photographic images to check grant eligibility (paragraph 1.4 and case studies 7 to 20).

9 But most tools used in government bodies are designed to detect fraud and error, rather than prevent incorrect transactions before they are paid. Detective data analytics try to find incorrect payments that have already been made. Preventative analytics aim to stop incorrect payments before they are made – and can be more cost-effective, as public bodies do not have to go through costly, time-consuming and often unsuccessful processes to recover money. Of the 14 uses of data analytics selected as case studies from public bodies, 11 are 'detective', two are 'preventative' and one has elements of both. The vast majority of the 28 data-sharing agreements set up to tackle fraud and error through the Digital Economy Act 2017 process were detective (paragraphs 2.4 to 2.6, case studies 7 to 20, and Figures 3, 4 and 6).

10 Savings so far have been modest compared to the amount potentially achievable. Some public bodies have achieved significant returns on their investment in data analytics to tackle fraud and error. For example, Network Rail reports a return on investment of 15:1 in its counter-fraud data analytics work and the NHS Counter Fraud Authority reports a 3:1 return on its use of analytics. But while most of our case studies could demonstrate positive results, public bodies could not always fully quantify the savings they had achieved, making it hard to quantify the overall success of government's use of data analytics. Officials told us that quantifying prevented fraud can be especially challenging as in some cases the measures put in place mean potentially incorrect transactions can never proceed to be identified and investigated. Overall, the scale of savings that we have seen have all been modest compared to both the scale of likely loss and the potential that counter-fraud officials see (paragraphs 1.4 and 2.7 to 2.9 and case studies 10 and 14).

11 There is no clear plan for how to realise the potential of data analytics to tackle fraud and error across government. At the Spending Review 2025, the government confirmed the £325 million additional funding per year by 2028-29 announced at Spring Statement to enhance counter-fraud capability in DWP and HMRC. GDS and HM Treasury also identified dozens of digital proposals from other departments with elements that, to varying degrees, related to fraud and error. Departments will now decide whether to fund these projects through their overall spending allocation. PSFA has relatively few levers over departments' use of digital resources and its strategy focuses on continuing existing initiatives. The GDS's blueprint for modern digital government sets out a more ambitious vision for digital transformation. But while it has set out its priorities, it has not yet translated them into an implementation plan or considered that plan from the perspective of fraud and error data analytics. Similarly, the other functions, such as GFF, have not set out their vision for how they will use data analytics to tackle fraud and error in their areas of responsibility (paragraphs 2.2, 2.3 and 2.8, and Figure 2).

12 We have identified ten challenges that government needs to overcome before it can realise more fraud and error savings through data analytics. We provide detail on the challenges in Part Two of the report. We have summarised the challenges, and made recommendations against them, on pages 8 and 9.

Conclusion

13 The use of data analytics to tackle fraud and error has demonstrated that it can achieve significant returns on investment, but to date the savings have been relatively modest compared to its overall potential and the value of taxpayer money lost to fraud and error. There is a clear mismatch between the scale of the problem of fraud and error and the lack of concrete plans to implement better data analytics. The PSFA needs to help government to step up to the challenge by working with departments and their arm's-length bodies to innovate and generate significant fraud and error savings. But it cannot do this alone. GDS needs to make sure its work facilitates fraud and error analytics, as this is such a significant component of its vision for achieving cost savings through digital government. Additionally, other functions need to acknowledge their responsibility to use and implement data analytics to help prevent waste.

We have identified 10 challenges to unlocking the potential of data analytics to tackle fraud and error, and associated recommendations

Challenge One: Providing cross-government leadership

- The Government Digital Service believes government could save as much as £6 billion a year by using data analytics to help tackle fraud and waste.
- Central government functions do not have a plan to support public bodies to fulfil this potential of data analytics to tackle fraud and error.

Recommendation 1

The Public Sector Fraud Authority (PSFA) should set out a plan for how it will support public bodies across government to make the best use of data analytics to tackle fraud and error. In putting this plan together, PSFA should engage with and consider the work of the Government Digital Service on 'modern digital government', and the work of other cross-government functions such as the Government Finance Function.

Challenge Two: Scaling up and replicating projects to focus on fraud prevention

- Preventative controls can be more effective than detective controls, but they are often more challenging to implement.
- Many pilots have not been scaled up to become business-as-usual or integrated as preventative controls.
- Currently, public bodies cannot easily replicate successful data analytics projects developed by others.

Recommendation 2

The Public Sector Fraud Authority should maintain a library of digital counter-fraud controls that public bodies can use to find ways to address their fraud risks. This should show the returns on investment that other public bodies have achieved through the controls.

Challenge Three: Making the investment case for data analytics

- It can be difficult for departments to make the business case for data analytics, due to short-term funding and the need for projects to pay for themselves quickly, poor information on savings and returns on investment, and the risk that some individual projects may fail to find savings so are best managed on a portfolio basis.
- Following the 2025 Spending Review, departments are deciding which fraud and error projects to fund as part of their overall spending allocation.
- New requirements on departments to better record fraud and error losses and returns should make it easier to calculate the benefit of using data analytics.

Recommendation 3

The Public Sector Fraud Authority (PSFA) and HM Treasury should develop a mechanism that allows public bodies to pool some of the costs, resources and savings associated with fraud and error data analytics. This might include PSFA managing a portfolio of seed funding in projects across government, with savings shared between the public body and the seed fund for use in future proposals.

Challenge Four: Making the most of central counter-fraud initiatives

- Cabinet Office offers a number of data analytics tools that are best provided centrally.
- There has not been widespread take-up of these central initiatives, such as the National Fraud Initiative, which compiles data to identify potentially fraudulent activity.
- Officials cited resourcing, understanding of the available initiatives, and the recharging models among the reasons for the poor take-up.

Recommendation 4

a) HM Treasury should make the use of the National Fraud Initiative mandatory and agree with the Public Sector Fraud Authority (PSFA) the criteria for where public bodies should use other centrally provided tools; and

b) HM Treasury and PSFA should review the charging model for PSFA central services to ensure they do not dissuade public bodies from making savings.

Challenge Five: Building controls into existing processes and new projects

- Tackling fraud and error requires a whole-organisation approach, but is sometimes seen as the sole responsibility of counter-fraud teams.
- Cross-government functions would need to work together more closely to fully unlock savings from fraud and error data analytics, by embedding fraud and error perspectives into government functional standards, finance and business processes and digital projects.

Recommendation 5

a) The Public Sector Fraud Authority should review government functional standards and 'NOVA' standardised functional processes to make recommendations to other functions for where and how they could better tackle fraud and error; and

b) The Government Digital Service should update its guidance on digital development processes to include counter-fraud and error perspectives as a key user, to ensure counter-fraud and error data and controls are built into new systems.

Challenge Six: Managing the key datasets

- Counter-fraud teams are not always aware of datasets that might help them tackle fraud and error.
- Government is seeking to improve the quality of some key datasets that have the potential to unlock better fraud and error analytics in future.
- Inconsistent data formats and systems make it harder to use data to tackle fraud and error.

Recommendation 6

The Public Sector Fraud Authority and the Government Digital Service (GDS) should maintain an overview of the key datasets required to support most fraud and error data analytics, and work with the bodies that maintain those datasets to create a mechanism enabling the sharing of quality and timely data that is consistent and in an understandable format. GDS should also set out how its ambitions in its blueprint and its existing work can help to reduce fraud and error, and set out an implementation plan to put these into place.

Challenge Seven: Managing the data-sharing process

- Sharing data is crucial for effective data analytics to tackle fraud and error.
- Public bodies continue to find it difficult and bureaucratic to share data to help tackle fraud, even though it is permitted under legislation.
- As more data is shared and systems linked, the risk increases that fraudsters penetrate one system to take advantage of another.

Recommendation 7

a) The Public Sector Fraud Authority (PSFA) and the Government Digital Service (GDS) should build on the Digital Economy Act 2017 data-sharing process to introduce a managed process to support public bodies to share data. This managed process should include an overview of the pipeline of potential agreements, standardised templates, clear decision points and key performance indicators around approval time;

b) PSFA and GDS should also advise public bodies on how to ensure clear ongoing governance arrangements over shared data to manage the risk of fraudsters gaining access to multiple systems through access to one; and

c) PSFA should further explore the use of non-government and private sector databases such as the fraud databases produced by Cifas.

Challenge Eight: Putting in place the right skills

- Effective use of data analytics to tackle fraud and error requires a blend of digital skills and fraud and error subject-matter expertise.
- Most of the successful data analytic projects we have seen have been developed by dedicated teams that bring these skills together.

Recommendation 8

The Public Sector Fraud Authority should work with the Government Digital Service to publish a playbook on how public bodies can develop the multidisciplinary team and capability to develop and deploy counter-fraud data analytics.

Challenge Nine: Optimising the staffing and algorithms to maximise the return

- Fraud and error data analytics tools often require staff to review flagged payments, but departments have not always resourced this to the optimal level to maximise returns.
- To maximise savings, public bodies also need to optimise algorithms to identify fraud and error and investigate the right number of 'risky' cases.

Recommendation 9

The Public Sector Fraud Authority and HM Treasury should encourage departments to keep their fraud and error data analytics under review, and optimise them accordingly to ensure that they are bringing the maximum fraud and error savings.

Challenge Ten: Maintaining public trust while harnessing new capabilities

- Public bodies must balance transparency about their use of data analytics with the risk of making it easier for fraudsters to take advantage.
- Officials also raised concerns that the legal inhibition of profiling individuals was preventing them from making full use of data analytics to fight fraud.

Recommendation 10

a) The Public Sector Fraud Authority should report to Parliament on whether it believes updated legislation is required to make the best use of data analytics to tackle fraud and error;

b) The Department for Science, Innovation & Technology (DSIT) and the Government Digital Service (GDS) should provide specific advice about how to best publish details about analytics tools to fight fraud and error on the algorithmic transparency records, given concerns around revealing control weaknesses; and

c) DSIT and GDS should encourage public bodies to report on the impact of data analytics on different customer groups.

Part One

How data analytics can tackle fraud and error

1.1 Fraud and error in the public sector generally means an incorrect amount of money has been paid out or received by government, or government has made a transaction with an incorrect or ineligible party. In this part we set out examples of how the public and private sector use data analytics to tackle fraud and error.

What do we mean by data analytics?

1.2 By data analytics we mean a range of different techniques and tools. **Figure 1** summarises the data analytic techniques that we saw being used by both the private and public sector to tackle fraud and error. Counter-fraud experts, within and outside of government, consistently told us that data analytics needed to be a key part of any plan to reduce fraud and error. Many projects use multiple techniques.

Figure 1
Types of data analytics used to tackle fraud and error

Data analytics refers to a wide range of techniques that can be used alone or in combination to tackle fraud and error

Technique	How it can be used to tackle fraud and error
Artificial Intelligence (AI)	The use of digital technology to create systems capable of performing tasks commonly thought to require intelligence. This often involves machine learning. This can be used in voice analytics, text analytics, image analysis and other tools.
Data matching	Linking multiple datasets to verify information or detect anomalies. This can include fuzzy matching techniques to link records that are approximately, but not exactly, the same.
Data-sharing	Sharing information within and between organisations to enable data matching and analysis.
Document verification	Using AI or data matching to detect the use of fraudulent documentation.
Image analysis	Using a computer programme, that can involve using AI, to find duplicate or similar images used to commit fraud.
Network analysis	Using data matching to find links between companies or individuals, to identify potential patterns and indicators of fraud – for example, payments to friends and families and connected companies.
Payee verification	Using data matching to check the details associated with a bank account match those being provided, to stop fraudulent payments from being made.
Text analytics	Using techniques to analyse and interpret text, which can include using AI, to identify suspicious patterns that may indicate fraudulent activity.
Risk scoring and data rules	Using available data and techniques such as statistics or predictive modelling to calculate a risk score or flag a case as worth investigating. This approach could also be completed on, for example, transactions, entities, or devices.
Voice analytics	Using techniques to analyse patterns of speech, which can include using AI, to detect risky patterns that might indicate potentially fraudulent activity.

Source: National Audit Office analysis of counter-fraud techniques seen in interviews and walkthroughs with organisations inside and outside of government

Examples of data analytics being used outside of the government

1.3 The use of data analytics is a well-established tool for reducing the cost of fraud and error in the private sector. We conducted interviews with organisations including banks, insurance companies, software providers and accountancy and audit firms, and talked to them about the data analytics techniques they use to tackle fraud and error. We have set these out below to illustrate the types of capability in the private sector, and do not endorse any particular provider. We have identified some common good practice themes from these examples.

- **A focus on the bottom line:** while some tools help private sector organisations meet their compliance requirements, they also protect profits by reducing money lost to fraud and error.
- **Prevention rather than detection:** private sector organisations attempt to stop fraudulent payments from going out by building data analytics into front-line controls.
- **Using risk scoring and data rules:** data analytics flag potentially fraudulent cases for human review, with higher risk scores subject to more scrutiny.
- **Taking a whole-case view:** tools bring together everything the business knows about the customer to help assess the risk.
- **Multilateral data-sharing:** data are shared between other businesses or organisations through third-party data-sharing tools to help assess the risk.

Banks told us they combined a variety of different analytics tools each designed to head off specific risks

1. Retail banking sector: Layering a suite of 'off-the-shelf' analytics tools

Types of analytics	Payee verification; data-sharing; data matching; risk scoring and data rules

Two banks showed us how they use several analytics tools to protect against fraud threats. They develop tools in-house and buy from other commercial providers. Some examples of tools they use are:

- **Payee verification and linked bank account checks:** off-the-shelf services such as those provided by SurePay, and 'TruValidate' Bank Verification, run by TransUnion, enable the bank to check that the receiving bank account details and name match before it processes a payment.
- **Fraud databases:** fraud databases flag instances of fraudulent conduct and and help banks to understand fraud risks for people applying to open accounts. These databases include Cifas' National Fraud Database (see case study 3), National Hunter, and Synectics Solutions' National SIRA.
- **Daily transaction monitoring:** internal data science teams monitor transactions and use rule-based tests to check for potential anomalous activity. For example, multiple small payments into one account may be flagged as potential 'tester' payments indicating the beginning of scam.

An insurance company showed us how it has introduced voice analytics to prioritise which claims to subject to more scrutiny

2. Clearspeed: AI-assisted voice analytics to prevent fraud

Types of analytics	Voice analytics; artificial intelligence (AI) (optional); risk scoring and data rules

Clearspeed provides an AI-assisted analytics tool which analyses vocal responses to an automated set of yes/no questions made via telephone and provides real-time outputs about possible fraud risks that could be investigated.

Clearspeed told us that its solution can accurately and quickly assess potential risk, and that it can help users to focus follow-up where fraud risk is flagged to drive efficiencies, reduce fraud, and deliver a better user experience. It believes its technology could, for example, help to improve efficiencies and prevent fraud and error in government procurement, grants, tax, and other services where government requires assurance over the validity and completeness of information it has been provided.

One major UK insurance company showed us how they had used Clearspeed to identify fraudulent claims that had not previously been flagged as risky. When the insurance company was testing the tool, it told us that 17 out of a sample of 100 claims that were not previously flagged as risky were found to be fraudulent. It said implementing the tool had saved it money and that customers had not raised concerns about using Clearspeed.

Private companies share and use information about previous instances of confirmed fraud

3. Cifas National Fraud Database (NFD): Reciprocal data-sharing to detect fraud

Types of analytics	Data-sharing; data matching

The National Fraud Database (NFD) is a not-for-profit tool, run by the not-for-profit fraud prevention organisation Cifas, which contains instances of confirmed fraud committed by individuals or companies from around 800 public and private sector organisations. While some local authorities use the NFD, only a handful of arm's-length bodies in government use it, and no central government departments use it. Users can, for example, conduct searches to help check grant recipients and to uncover instances of identity fraud, false insurance claims and blue badge misuse, among other types of fraud. They can then use this information to help prevent fraud against their own organisation.

The database depends on reciprocity, with organisations needing to submit their own data on fraud to the database as part of the access agreement. Cifas oversees the scheme rules and monitors compliance to ensure that instances of fraudulent conduct filed to the database meet the required evidence standards.

Large software providers offer 'off-the-shelf' tools to identify suspicious activity such as inflated procurement bids

4. Software provider: Anti-bid rigging tool

Types of analytics	Artificial intelligence (AI); text analytics; risk scoring and data rules

A large software developer showed us a tool it has developed which uses text analytics and AI to identify potential procurement fraud. Using machine learning 'trained' on past cases of procurement fraud, the tool examines bid structures and prices for patterns that might indicate fraudulent bidding practices for investigation. The software provider aims for the tool to help bodies to bolster counter-fraud controls in procurement, particularly to prevent bid rigging in large-scale infrastructure or schemes with complex procurement processes.

Data analytics can also be used to understand the risk represented by the device being used to make a transaction

5. LexisNexis 'ThreatMetrix': Network analytics for risk scoring of 'digital identities'

Types of analytics	Data-sharing; data matching; risk scoring and data rules; network analysis

LexisNexis Risk Solutions has developed ThreatMetrix, a globally shared network analytics tool that brings together fraud intelligence from analyses of billions of transactions, device IDs, email addresses and phone numbers to understand potential risk associated with individuals transacting online.

LexisNexis told us that ThreatMetrix uses such intelligence to determine individuals' digital footprints and flag any suspicious activity. Risk factors include the age of an email account, how and where a device is being used, mouse movements that suggest cut and paste actions at login, and the detection of bots used to automatically fill in forms and details online. LexisNexis told us that banks, financial services and other sectors deploying the tool can decide, based on their risk appetite, what type of flags will automatically block transactions or initiate further verification or investigation.

Banks now share real-time data to allow them to trace transactions across the UK financial system

6. Vocalink: Network analysis and transaction risk scoring for the banking sector

Types of analytics	Network analysis; data-sharing; data matching; risk scoring and data rules

Vocalink provide the technical infrastructure required to run the UK's retail interbank payment systems. This includes the Bacs, Faster Payments and the Image Clearing System owned and operated by Pay.UK. Vocalink told us that it uses data matching, network analysis, and instantaneous transaction risking to help the many banks that use its services to detect and prevent fraudulent payments. It told us 'Multilateral' sector-wide sharing via Vocalink enables banks to assess risk using more data than they have individually and that this allows banks to work together, for example, to stop fraudsters paying out money through chains of UK accounts that they control. Vocalink estimates it has helped contribute to preventing over £100 million a year in losses since 2023 through stopping payments that were authorised by potential victims of scams, before the payments reached the fraudsters.

Examples of data analytics being used within government

1.4 We asked finance directors of government departments to provide examples of data analytics they were using or developing to detect or prevent fraud and error, and interviewed counter-fraud teams involved in these projects. We saw a wide range of data analytics techniques and analysis being used or developed, from simple data-sharing and data matching to deep learning and artificial intelligence (AI). We identified the following themes.

- **Some public bodies use well-established data analytics tools:** HM Revenue & Customs and the Department for Work & Pensions have been using techniques like data matching for a long time as part of their counter-fraud efforts.
- **Other public bodies are experimenting with innovative tools:** Public bodies like the Department for Transport and HM Prison and Probation Service are piloting AI and machine learning to tackle fraud and error.
- **Low take-up of newer tools:** Public bodies have developed innovative data analytics tools for use internally but only when resources have allowed.

- **Detection rather than prevention:** Most of the analytics were detective controls, as opposed to preventative.
- **Moderate savings compared to potential:** In theory, with good-quality linked data, these technologies can deliver more immediate returns on investment tackling fraud and error without requiring the wider system or organisational reform that fuller digital transformation would require. However, many public bodies struggled to quantify savings, which often remained modest compared to the overall potential and losses from fraud.

HM Revenue & Customs (HMRC) joins up over 100 datasets using its network analytics tool to identify additional tax revenue

7. HMRC: Data matching tool to find tax fraud — Detective

Types of analytics	Status	Savings	Introduced
Data-sharing; data matching; network analysis; risk scoring and data rules	Business-as-usual	£3 billion to £4 billion a year	2010

HMRC uses a number of in-house data analytics platforms to help decide where it should prioritise tax investigations, and to support those investigations. The platforms it currently uses, one of which was first introduced in 2010, now bring together over 100 datasets to find potential anomalies between an individual's declared income and their assets or lifestyle.

HMRC told us that it has started to take a more responsive approach when using its data analytics tools, so that it can create smaller, targeted networks of individuals (rather than relying on a single network that contains all the data available) and tackle specific fraud risks more efficiently. It provides a shared data service to support its internal teams, which develop data analytics tools and 'clean' datasets to reduce false positives (non-fraudulent instances incorrectly flagged as fraudulent) and improve anomaly detection. It told us it can take a 'fail fast' approach as it has the resources and culture to support trial and error in data analytics development before committing to full-scale rollout.

The Department for Work & Pensions (DWP) is using data analytics to prioritise which cases to review

8. DWP: Targeting incorrect benefit payments — Detective

Types of analytics	Status	Savings	Introduced
Risk scoring and data rules	Funded to 2029-30	>£1 billion	2022

DWP uses data analytics to identify potentially incorrect Universal Credit payments. Universal Credit claims that are flagged as risky are sent to case workers to review whether there may have been previous incorrect payments, and to correct future payments. DWP also looks to use the insights from this 'Targeted Case Review' to strengthen its preventative controls. Between 2022-23 and 2024-25, DWP reviewed around 1.15 million cases, correcting claims as needed. DWP estimates that correcting these claims has already saved it around £581 million, and that it will save a similar amount through stopping the benefit overpayments that would have otherwise been made on these claims in the future. DWP plans to further develop its approach to Targeted Case Review and the types of analytics it performs, so it can better target incorrect payments.

HM Revenue & Customs (HMRC) has introduced an option for people to use open banking data to verify their bank accounts and enable faster payments

9. HMRC: Verifying payee banking details

Preventative

Types of analytics	Status	Savings	Introduced
Payee verification; data-sharing; data matching	Business-as-usual	Unquantified	2018 initially 2024 for Pay As You Earn (PAYE)

HMRC uses a payee verification tool to check that repayments are going to the right taxpayer. The tool checks that the account details provided to HMRC for a repayment match the details held by UK banks, providing assurance that repayments are not being fraudulently redirected to the wrong bank account.

In 2024, HMRC introduced an open banking option for people owed a PAYE refund. It allows those owed a refund to give consent to HMRC's open banking provider for a one-off access to their account details so HMRC can verify it is a real bank account and make a direct payment instead of sending a cheque (which had a cost associated with it). The provider does not store or share any of the data and HMRC cannot see customers transactions or online bank accounts. HMRC told us that 1.5 million customers have used the new service to date, and that it expects the use of open banking instead of cheques to bring an efficiency saving of £2.5 million in the first year, as well as meaning that taxpayers receive repayments more quickly.

The NHS Counter Fraud Authority (NHSCFA) has recently invested in its general data analytic capability so that it can review fraud and error risks across different parts of the NHS

10. NHSCFA: Machine learning and data science pilot to detect fraud in NHS spending

Detective

Types of analytics	Status	Savings	Introduced
Artificial intelligence (AI); risk scoring and data rules	Pilot	£10 million to £100 million (expected)	2024

The NHSCFA introduced Project Athena, a data science and machine learning project, as a pilot in early 2024 to provide new counter-fraud capability that will contribute to tackling fraud in the NHS. The pilot detects anomalous data points that could be prioritised for investigation or fraud prevention intervention, such as staff working elsewhere while claiming to be sick or fake invoices for good and services not supplied. Health experts provide contextual information to reduce false positives. NHSCFA told us that it is currently achieving a 3:1 return on investment, in part due to Project Athena.

The Department for Work & Pensions (DWP) uses data-sharing and data matching to flag ineligible claims

11. DWP: Data-sharing and data matching to check eligibility for benefits

Detective

Types of analytics	Status	Savings	Introduced
Data-sharing; data matching; risk scoring and data rules	Business-as-usual	>£100 million	2018

DWP uses real-time information provided by HM Revenue & Customs, through the 'Verify Earnings and Pensions Service' (VEPS), about the income and employment status of people who receive various benefits, including Carer's Allowance. While benefit claimants are responsible for reporting their income to DWP, VEPS provides DWP with the capability to verify a claimant's earnings before approving new benefit claims where it considers this is required. VEPS also provides alerts about changes in earnings that may not have been reported, so DWP can investigate whether a claimant's income has risen above the eligibility threshold to receive certain benefits, including Carer's Allowance.

DWP pays Carer's Allowance based on eligibility criteria that both the carer and the person being cared for must meet. DWP staff investigate some VEPS cases to check details, such as income and allowable expenses, and this can include corresponding with claimants by text, letter or phone. DWP staff assess and decide whether payment of Carer's Allowance should continue and what action is needed to recover any overpayment.

In 2024 we reported that DWP had investigated around half of available VEPS cases relating to Carer's Allowance per year since 2020-21 and that DWP estimates it saved £121 million from 2018-19 to 2023-24. As part of the 2025 Spending Review, DWP has secured funding to invest in VEPS and deploy additional resources to work through the alerts it has yet to review, and the alerts it expects to receive in the future.

The Department for Transport (DfT) has piloted the use of deep learning to identify whether people are using pictures of the same charger to make multiple grant claims

12. DfT: AI image detection for grant fraud

Detective

Types of analytics	Status	Savings	Introduced
Artificial intelligence (AI); image analysis; risk scoring and data rules	Completed pilot	<£100,000	2024

DfT has developed an image recognition tool to combat fraud risks in a grant scheme that funds the installation of electric vehicle charging points. DfT identified that the same image or multiple images of the same charger could be fraudulently submitted as evidence for multiple grant claims. The department's counter-fraud team worked with its data scientists to develop an AI tool using deep learning to quickly identify similar images for investigation. DfT has so far identified and recovered small amounts of fraudulently obtained funding and has blocked further dealings with fraudulent vendors. DfT has told us it has now started to use the tool in other grant schemes, and is considering how it can integrate live data into the tool to prevent fraud.

The Department for Education (DfE) uses data-sharing and data matching to check that apprenticeship funding relates to people who are employed

13. DfE: Data-sharing to detect apprenticeship fraud

Detective

Types of analytics	Status	Savings	Introduced
Data-sharing; data matching; risk scoring and data rules	Business-as-usual	£100,000 to £1 million	2020

DfE funds training providers to deliver apprenticeship training to employed individuals, with providers required to confirm that the apprentices are in employment. DfE shares apprenticeship record data with HM Revenue & Customs (HMRC), and HMRC matches this with its own Pay As You Earn (PAYE) employment data to identify training providers claiming funds for apprentices not recorded as being in work.

The project is based on a Digital Economy Act 2017 data-sharing pilot, which DfE has developed and continued as business-as-usual. DfE initially shared data in a pilot with HMRC in 2020 by uploading a secure file to the HMRC platform which, once populated by HMRC, was downloaded back to DfE restricted folders. This identified small amounts of fraud and error. DfE now has a more sophisticated data-sharing arrangement with HMRC, and since the introduction of regular access to HMRC data in August 2024 it has used this to check over 250,000 new apprenticeships. DfE is now planning further work relating to 7% of the apprenticeships checked in this way, to understand whether the individuals could not be confirmed through HMRC PAYE information because of data mismatches, or because of fraud and error.

Network Rail uses data analytics to identify procurement anomalies and brings these together in a dashboard

14. Network Rail: Dashboards to detect procurement fraud

Detective

Types of analytics	Status	Savings	Introduced
Data-sharing; risk scoring and data rules	Business-as-usual	£100,000 to £1 million	2024

Network Rail has developed dashboards to bring together data on money spent across the organisation, showing the level of fraud risk for each area of spending. Network Rail uses the dashboards to highlight anomalies like a fuel card being used twice in a day. The finance team provides context and root cause information on any anomalies, and the counter-fraud team investigates cases where there is a risk of fraud, prioritising based on the size of the payment. The dashboards were developed using, and in response to, Network Rail's fraud risk assessments, which identified procurement processes most susceptible to fraud.

Network Rail partly relies on external data from suppliers. Suppliers do not automatically transfer data in real-time but instead send periodic updates that refresh Network Rail's dashboards at different intervals for different suppliers. Tools such as these could be optimised through automatic transfer of data, but this would require additional resources to develop.

Overall, Network Rail reports a return on investment of 15:1 in its counter-fraud data analytics work.

The Department for Education (DfE) is using network analysis to identify links between those receiving DfE funding and other directors and firms, to support fraud investigations

15. DfE: Director Network Analysis and fraud risk scoring

Detective

Types of analytics	Status	Savings	Introduced
Network analysis; data-sharing; data matching; risk scoring and data rules	Proof of concept	£100,000 to £1 million	2024

DfE used data matching and network analysis to create the 'Director Network Analysis' tool, which identifies links between individuals or companies receiving DfE funding with other directors and firms, to help support fraud investigations. As part of this, DfE is also introducing rankings of training providers' risk based on their links to high-risk individuals or providers. DfE's intelligence and data team is embedded in the department's counter-fraud team. This helped DfE to ensure it had the required expertise to develop and implement this tool.

The Ministry of Justice (MoJ) is using machine learning to understand its internal fraud and corruption risks

16. HM Prison and Probation Service (HMPPS): Machine learning to detect internal fraud

Detective

Types of analytics	Status	Savings	Introduced
Artificial intelligence (AI); text analytics; data-sharing; risk scoring and data rules	Business-as-usual	£10,000 to £100,000	2024

The MoJ data science team developed a machine learning model that flags possible fraud, corruption and bribery using HMPPS staff misconduct records. It has led to improved and more streamlined fraud reporting that identifies key themes and risks that counter-fraud staff can prioritise, and has saved time and resources.

The model was trained on thousands of staff misconduct records, including investigations and disciplinary cases across multiple sites. It analyses free-text summaries and details of allegations to assign labels for types of fraud, corruption and bribery. This used to be a manual task but has now been semi-automated by the model. The data science team plans to extend similar analysis across the MoJ.

The Legal Aid Agency (LAA) has used data-sharing and data matching to speed up its counter-fraud investigations

17. LAA: Data-sharing and data matching with HM Revenue & Customs (HMRC) to prevent fraud

Preventative

Types of analytics	Status	Savings	Introduced
Data-sharing; data matching; risk scoring and data rules	Pilot	<£1 million	2023

LAA used the Digital Economy Act 2017 to provide a legal gateway to pilot data-sharing with HMRC, to verify whether legal aid applicants were eligible for legal aid. During the pilot, LAA provided HMRC with the details of around 600 recipients whom LAA suspected were making fraudulent claims. HMRC matched those recipients to income data and shared this with LAA. LAA investigated recipients who didn't meet income eligibility requirements and estimates that it has saved around £500,000 in future erroneous payments.

LAA officials told us senior stakeholders at the organisation bought into the pilot because, otherwise, investigators may have spent significant time verifying each recipients' income, whereas the HMRC data check takes minutes.

The pilot ran from March 2023 to March 2024, and LAA is now seeking to move this pilot to a business-as-usual data share with HMRC.

The Public Sector Fraud Authority (PSFA) is developing a single network analytics platform ('SNAP') that brings together data on companies for the use of all government departments

18. PSFA: Network analysis to assess fraud risk of UK companies and directors

Detective

Types of analytics	Status	Savings	Introduced
Network analysis; data-sharing; data matching; risk scoring and data rules	Supporting Bounce Back Loan (BBL) scheme recoveries – business-as-usual SNAP – Rollout and continuous development	>£100 million	Supporting BBL scheme recoveries – 2021 Developed into SNAP – 2024

PSFA is developing a network analysis tool that brings together data on companies, which it intends for all government departments to eventually use. The tool, called the Single Network Analytics Platform (SNAP), uses public and non-public government datasets to provide government with a clear picture of UK-registered companies. PSFA developed SNAP while it was supporting the Department for Business & Trade with COVID-19 BBL scheme analytics. PSFA has reported that, by March 2023, around £268 million had been saved through this data analytics work. These savings were achieved, for example, by identifying companies that were being fraudulently dissolved to avoid paying back BBLs. PSFA expects to report a continued significant impact from SNAP going forward.

PSFA brings data into SNAP in batches and matches it to data already held in the platform. SNAP provides users with instant risks scores and information on links between companies and their directors, so that users can understand potential fraud risk.

The Public Sector Fraud Authority (PSFA) operates the National Fraud Initiative (NFI), which is the largest fraud and error sharing exercise across the public sector

19. PSFA: National Fraud Initiative

Detective | Preventative

Types of analytics	Status	Savings	Introduced
Data-sharing; data matching	Business-as-usual	>£1 billion	1996

PSFA operates the NFI, a long-standing data-sharing and matching service. NFI includes a range of services that prevent and detect fraud. The national exercise (every two years) element compares more than 8,000 datasets from central government public bodies, local authorities and private sector organisations to identify data inconsistencies that may indicate fraudulent activity. Local authorities are mandated to use the NFI and share data on things such as housing benefits, council tax, payroll and Right to Buy. NFI participants can also do preventative checks at the point of application – for example for housing benefit claims or applications for employment. From 1 April 2022 to 31 March 2024, NFI generated UK-wide savings of £480 million, and around £1.8 billion since 2015.

The British Council uses dashboards to understand the risk from non-compliance with its internal policies

20. British Council: Dashboard to monitor compliance with internal policies

Detective

Types of analytics	Status	Savings	Introduced
Risk scoring and data rules	Business-as-usual	£10,000 to £100,000	2023

The British Council Finance Policy and Governance team developed a dashboard to analyse compliance with travel and expense related policies across the organisation. The dashboard is used to manage areas identified as high risk, such as purchasing cards. It flags non-compliance for investigation and monitors trends to highlight areas that might need additional controls.

The dashboard has decreased non-compliance: for example, the British Council has reported a 30% reduction in the use of corporate credit cards for personal use and a 50% reduction in instances of staff breaching the travel and expense cost limits. The team initially faced data availability and quality issues and needed to integrate data from other systems.

Part Two

The strategic challenges

2.1 We spoke to counter-fraud and error teams and data analysts across public bodies to understand the challenges they faced and how their work could be better supported. Below are our observations based on these conversations about the biggest challenges to the more widespread use of data analytics to tackle fraud and error.

Challenge One: Providing cross-government leadership

2.2 The Government Digital Service (GDS) believes the government could save as much as £6 billion a year by using data analytics to help tackle fraud and waste. GDS produced its estimate of £6 billion to give an indication of the potential savings. It based this on the savings that the Department for Work & Pensions (DWP) has achieved in one example of data analytics and applied these savings to the Public Sector Fraud Authority's (PSFA's) estimate of the level of fraud and error across all of government. This implies that most of the savings would come from tax and benefits (which already use data analytics), but also that a significant amount would come from the rest of government. However, the estimate does not take account of the cost or effort needed to achieve the savings, or what needs to happen for such savings to be delivered, and as such should be read with caution.

2.3 Central government functions do not have a plan to support public bodies to fulfil the potential of data analytics to tackle fraud and error.

- The Government Counter Fraud Function, led by the PSFA, has a functional strategy for 2024-2027 that commits it to harnessing data and technology more effectively.[2] To date, it has focused on enhancing its central offer, promoting pilots of new counter-fraud technology and working on a common framework for data-sharing. But it has relatively few levers over departments' use of digital resources and its strategy focuses on continuing existing initiatives.

2 The Public Sector Fraud Authority and Government Counter Fraud Function, *The Government Counter Fraud Functional Strategy 2024-2027*, March 2024 (viewed on 25 June 2025).

- The GDS 'blueprint for modern digital government' sets out a more ambitious vision for digital transformation, of which the use of data analytics to tackle fraud and error is a part.[3] But while it has set out its priorities, it has not yet translated them into an implementation plan or considered that plan from the perspective of fraud and error data analytics.
- The other functions, such as the Government Finance Function have not set out their vision for how they will use data analytics to tackle fraud and error in their areas of responsibility (**Figure 2**).

Figure 2

Central government plans to support better use of data analytics to fight fraud, as at June 2025

There are several central government strategies relevant to tackling fraud and error through better use of data analytics

Organisation/Function	Strategy	Key points
Public Sector Fraud Authority (PSFA)	Government Counter Fraud Functional Strategy 2024-2027	By 2027 the Government Counter Fraud Function, which is led by PSFA, aims to: ● have more key datasets in accessible and shareable forms; ● increase the use of technology and data analytics, including AI, to increase the amount of fraud prevented and detected; ● increase uptake of PSFA's Single Network Analytics Platform and the number of data-sharing pilots under the Digital Economy Act 2017; ● continue to maintain the National Fraud Initiative; and ● identify opportunities to work with the private sector to harness data and technology more effectively.
Government Digital Services (GDS)	A blueprint for modern digital government	GDS aims to combat fraud through better data-sharing and stronger counter-fraud capabilities, delivering this in part by: ● taking a new approach to digital funding with HM Treasury to realise efficiencies and productivity gains including through tackling fraud and waste; and ● creating a National Data Library and establishing a 'once only' rule, meaning that people's data can be reused by other public bodies with appropriate safeguards. This is intended to build on existing work by GDS.
Government Finance Function (GFF)	GFF Strategy 2030	GFF aims to work with other functions to: ● bring multiple datasets together with finance data to produce greater insights; ● use the expertise of the Digital and Data Function in GDS to identify the most effective tools to analyse and present data; and ● work across organisational boundaries to identify and collect performance data to improve decision-making and achieve better outcomes.

Note

1 A function is a grouping aligned across government to manage functional work such as human resources, commercial, or finance. Functions are embedded in departments and arm's-length bodies. PSFA leads the Government Counter Fraud Function. GDS leads the Government Digital and Data Function. GFF is led by a central Government Finance Function team in HM Treasury.

Source: National Audit Office analysis of Public Sector Fraud Authority, Government Digital Services and Government Finance Function strategies and plans

3 Government Digital Service, *A blueprint for modern digital government,* CP 1252, January 2025.

Challenge Two: Scaling up and replicating projects to focus on fraud prevention

2.4 Preventative controls can be more effective than detective controls, but they are often more challenging to implement (**Figure 3**). Integrating preventative controls into existing business processes often requires real-time data-sharing and cleaning of data for the controls to flag or stop potentially incorrect payments. Detection occurs after a payment is made and does not require real-time data-sharing, but does require public bodies to go through costly, time-consuming and often unsuccessful processes to recover money. Most data analytics tools we have seen in government are to detect potentially incorrect payments that have already been made, and the tools are not part of front-line preventative controls. Additionally, the vast majority of the 28 data-sharing agreements set up to tackle fraud and error through the Digital Economy Act 2017 process were detective controls.

Figure 3
Comparison of preventative and detective data analytics

Preventative controls are more effective because they stop incorrect payments before they occur, but they can be harder to integrate into existing business processes

	Typical features of preventative measures:	Typical features of detective measures:
What is its objective?	To stop incorrect payments before they occur.	To detect incorrect payments after they have occurred.
Who does it?	Operational teams have data analytics to confirm eligibility integrated into their processes.	Separate fraud or compliance teams use data analytics to confirm eligibility of previous payments.
When is it done?	Operational staff investigate flagged transactions before payment is made.	Fraud or compliance staff investigate a selection of flagged past payments, while payments are continuing.
What happens if it is not properly resourced?	Flagged issues that are not resolved may delay correct payments.	Flagged issues that are not resolved may mean incorrect payments continue.
What data are required?	Requires real-time data-sharing and analysis.	Data extracted from standard systems at a point in time, normally analysed later.
How does it achieve savings?	Disrupts all incorrect payments caught by the measure. Pursuit and recovery is not needed.	Requires pursuit and recovery of past ineligible payments. May enable disruption of future incorrect payments where issues are detected.
Can it tell you additional information?	Tells you little about unknown problems.	Can aid root cause analysis of previously unknown problems.
Does it require changes to existing systems?	May require modification of existing systems or the need to build new systems.	Requires data to be extractable from existing systems.

Source: National Audit Office analysis of counter-fraud techniques

2.5 Many pilots have not been scaled up to become business-as-usual or integrated into processes as preventative controls. To scale up a project, public bodies need to be able to manage challenges around increased organisational complexity (pilots may not pick up more complicated cases), a lack of organisational readiness (e.g. legacy systems and change resistance), and increased governance (especially over data quality, security and privacy concerns). In the 28 fraud-related pilots since the Digital Economy Act 2017, only four had transferred to business-as-usual by June 2025 (**Figure 4**).

2.6 Currently, public bodies cannot easily replicate successful data analytics projects developed by others**.** We saw examples of different public bodies developing similar solutions for similar counter-fraud risks, but there is no available library of tools and examples of previous successful implementations for similar fraud and error risks. Such a library could build on the PSFA's post-event assurance toolkit, which highlights some of the products available to public bodies to tackle fraud and error but does not go into specific counter-fraud controls.

Figure 4

Outcome of data-sharing pilots under the Digital Economy Act 2017 fraud powers, as at June 2025

Most fraud data sharing pilots have not progressed into business-as-usual (BAU) data-sharing between public bodies

Status of pilot	Number of pilots
Currently active	3
Complete but not currently progressed to BAU	8
Complete and progressed to BAU	4
Associated with one-off spending	13
Total	**28**

Notes

1 Analysis excludes data-sharing pilots with devolved bodies (e.g. Scotland and Wales) and between local government bodies, but includes sharing between central government and local government bodies.

2 Pilots associated with one-off spending (e.g. COVID-19 and energy support schemes) would not normally result in a pilot moving to BAU, as the spending is not expected to become part of ongoing government spending.

Source: National Audit Office analysis of Digital Economy Act 2017 pilots, in conjunction with the Public Sector Fraud Authority

Challenge Three: Making the investment case for data analytics

2.7 It can be difficult for departments to make the business case for data analytics due to short-term funding and the need for projects to pay for themselves quickly, poor information on savings and returns on investment, and the risk that some individual projects may fail to find savings so are best managed on a portfolio basis. The cost of data analytics can vary, with some projects requiring sustained financial commitment and others requiring very little. But officials told us that they found it harder than it should be to make the case for data analytics, due to:

- **short-term funding and the need for projects to pay for themselves quickly:** Officials told us that the payback periods from setting up counter-fraud data analytics have not always aligned with the short-term spending review funding agreements of recent years, making it difficult to make the case for investment. The 2025 Spending Review provided a three-year funding allocation, with four departments quoting that they wanted to achieve fraud and error savings within this period as part of their efficiency plans;[4]

- **poor understanding of the return on investment:** Public bodies generally have poor data on the amount of fraud and error they face. Few parts of government estimate their fraud and error losses, and counter-fraud practitioners told us they struggle to meet existing requirements around reporting detected fraud. Understanding and reporting prevented fraud is more challenging still, as in some cases the measures put in place mean a potentially incorrect transaction can never proceed to be identified and investigated. Without a solid understanding of the amount lost to fraud and error, it is difficult for public bodies to estimate how much could be saved through counter-fraud and error controls; and

- **public bodies alone are often not well placed to innovate in the way that is required to tackle fraud and error:** Tackling fraud and error requires innovation and some risk taking. Activities will not always deliver the expected savings because they are looking to detect and prevent something that is hidden, and a fear of limited returns on investment constrains some organisations from innovation. Innovation can be easier in organisations with larger counter-fraud functions, as they may be able to trial several new projects without impeding business-as-usual activity and still deliver savings across their portfolio of work, even if some innovative projects fail to bring the anticipated returns.

4 HM Treasury, *Spending Review 2025: Departmental Efficiency Plans*, June 2025 (viewed on 25 June 2025).

2.8 Following the 2025 Spending Review, departments are deciding which fraud and error projects to fund as part of their overall spending allocation. At the 2025 Spending Review, the government confirmed the £325 million additional funding per year by 2028-29 announced in the 2025 Spring Statement to enhance counter-fraud capability in DWP and HM Revenue & Customs (HMRC). At the time of publication, there were no further announcements of funding specifically for fraud and error data projects. Through the Spending Review, the Digital and Data Function (led by GDS) worked with HM Treasury to assess digital projects, including evaluating data-sharing and quality, skills and resources, technology requirements and alignment to digital delivery best practice. This work identified dozens of digital proposals with elements that, to varying degrees, related to fraud and error and departments will now decide whether to fund these projects through their overall spending allocation. At the time of publication, GDS analysis of approved initiatives with counter-fraud as a core objective or wider benefit, was underway but not yet completed.

2.9 New requirements on departments to better record fraud and error losses and returns should make it easier to calculate the benefit of using data analytics. HM Treasury now requires departments to include evidence-based estimates of the level of fraud and error for spend that is both 'significant to the organisation' and at 'significant risk of fraud and error' in their annual reports and accounts. Additionally, PSFA now agrees targets with departments for their fraud and error savings, and expects departments to report against this target. This information should help departments to demonstrate the potential of data analytics to make savings and help make the case for further activity.

Challenge Four: Making the most of central counter-fraud initiatives

2.10 Cabinet Office offers a number of data analytics tools that are best provided centrally (**Figure 5**). Providing central tools in this way can save public bodies from having to develop platforms, assemble data and cleanse data individually. Some of the initiatives, such as the National Fraud Initiative, are more effective if more organisations participate and share their data.

2.11 There has not been widespread take-up of these central initiatives (Figure 5). Use of these initiatives is voluntary for central government public bodies in England. Technologies like payee verification are well-established standard controls in the private sector, but in central government only HMRC uses the Crown Commercial Services commercial agreement to procure the payee verification service as part of its 'business-as-usual' practices – although some other parts of government are now exploring it. PSFA is rolling out its Single Network Analytics Platform (SNAP) to central government bodies gradually, so it is not yet meeting its full potential.

2.12 Officials cited resourcing, understanding of the available initiatives, and the recharging models among the reasons for the poor take-up. Counter-fraud teams told us that:

- implementing central initiatives, and integrating them into existing processes, takes time and requires additional resources;
- there was sometimes limited knowledge of what central initiatives are available, how they might be used, and the potential benefits; and
- government's use of recharging models for central services, meaning public bodies have to pay to make use of services, can act as a barrier to entry where the return on investment is uncertain.

Figure 5

Central government initiatives to support public bodies to tackle fraud and error, as at June 2025

Public bodies have not widely taken up central government initiatives

Central initiative	Description	Provided by	Extent of use	Cost to user
National Fraud Initiative (NFI)	Data-sharing and matching service used to identify data inconsistencies that may indicate fraud.	PSFA	36 central government bodies took part in 2024-25.[1]	£1,265 for the biennial National Exercise.[2]
Single Network Analytics Platform (SNAP)	Data-sharing, data matching and network analysis tool that provides risk scores for UK-registered companies.	PSFA	Four central government bodies.[3]	Tiered costs of between £25,000 and £75,000 per year, depending on size of public body.
Payee Verification	Data matching to check that the details associated with a bank account match those being provided, to stop fraudulent payments from being made.	Crown Commercial Services commercial agreements[4]	HM Revenue & Customs, with some other parts of government exploring use.	Varies depending on requirements and size of public body.
Spotlight	Tool that checks grant and contract eligibility for companies and charities by automatically performing due diligence checks through matching to relevant internal government data and external data sources.	Government Commercial and Grants Management Function	20 central government bodies.[5]	Between £5,000 and £56,000 depending on the size of public bodies and number of licences required.

Notes

1 This refers to the National Exercise conducted every two years. In the previous National Exercise, commencing in 2022-23, 22 central government bodies in England participated. These numbers include arm's-length bodies.

2 The cost data for NFI are for the National Exercise, which includes payroll and trade creditor datasets. There are also additional exercises like mortality screening that are available for an extra charge.

3 PSFA aims for six central government bodies to use SNAP by the end of the 2025-26 financial year.

4 Crown Commercial Services also provide commercial agreements that allow public sector bodies to procure counter-fraud audit and assurance services and debt resolution services for fraud recovery.

5 The extent of use for Spotlight listed includes government departments and arm's-length bodies from England only. The Government Commercial and Grants Management Functions are looking at options to make Spotlight functionality available through the Central Digital Platform for all public sector bodies.

6 There are over 400 central government public bodies in England, not all of which are large enough or function in a way that would benefit from participation in some of the central initiatives.

Source: National Audit Office analysis of central government initiatives

Challenge Five: Building controls into existing processes and new projects

2.13 Tackling fraud and error requires a whole-organisation approach, but is sometimes seen as the sole responsibility of counter-fraud teams. Building robust controls into existing processes requires data analytics as part of front-line operations, requiring a joined-up approach from digital, data analytics, finance and operational staff.

2.14 Cross-government functions would need to work together more closely to fully support public bodies to unlock savings from fraud and error data analytics, by embedding fraud and error perspectives into:

- **government functional standards:** The grants function specifies counter-fraud and error controls in its function, but counter-fraud officials told us that other functional standards could highlight where other disciplines can help tackle fraud and error;
- **finance and business processes:** For example, the Government Finance Function led a cross-functional programme to create 'NOVA', which acts as a repository of processes and controls for finance, procurement, grants and HR functions across government, and aims to standardise these. While NOVA incorporates controls that look to minimise waste, the PSFA and other cross-government functions have not worked together to ensure NOVA best enables preventative fraud controls; and
- **digital projects:** We have previously advised public bodies to create clear plans for up-front data requirements.[5] Projects could treat tackling fraud and error as a key user group. This is necessary because the way data are collected and structured is determined early on in a project and this can affect whether data analytics tools can later be used to best effect.

5 National Audit Office, *Digital transformation in government: A guide for senior leaders and audit and risk committees*, February 2024.

Challenge Six: Managing the key datasets

2.15 Counter-fraud teams are not always aware of key datasets that might help them tackle fraud and error. There are datasets that are particularly helpful for tackling fraud and error across government, such as HMRC data on employment income. However, counter-fraud officials told us they are sometimes unaware of data within their own departments, and in other public bodies, that could be used to fight fraud and error.

2.16 Government is seeking to improve the quality of some key datasets that have the potential to unlock better fraud and error analytics in the future. This includes the following:

- **Companies House data:** Data on UK-registered companies, including names and correspondence addresses of company directors, registered company addresses and incorporation dates can be vital to tackle company-related fraud. However, Companies House has not traditionally verified data on its register and the Committee of Public Accounts concluded that it was undermined by errors and fake entries.[6] We have also reported that Companies House previously had limited scope to share its data to support cross-government counter-fraud work.[7] In March 2024, the first measures under the Economic Crime and Corporate Transparency Act 2023 came into force, including the ability to proactively share information with other government departments and law enforcement agencies. The new measures also included new powers to check information for company registrations, request evidence and remove inaccurate information. Companies House is now improving its data and is working on plans to introduce real-time data in the future.

- **Procurement data:** Being able to track the progress of procurement exercises, and to identify buyers and suppliers in a systematic way and link them to financial information, allows anomalies to be identified. The Open Contracting Partnership (OCP) lists 73 red flags for detecting fraud and corruption, such as where contract transactions exceed the contracted amount. Until recently, the UK has not been able to use these flags due to the way it organised its procurement data. The Procurement Act 2023 legislates for increased transparency and publication requirements, and alongside this the Government Commercial Function has introduced a new Central Digital Platform that better organises procurement data and provides unique identifiers for buyers, suppliers and contracts. The OCP believes this will enable 43 of its 73 red flags to be calculated. Cabinet Office aims to further improve procurement data by linking spending data to contracts, to make it possible to identify how much is spent with each supplier. It also intends to provide a suite of dashboards and analytics to enable open analysis of commercial data in the future.

6 Committee of Public Accounts, *Department for Business, Energy & Industrial Strategy Annual Report and Accounts 2021–22*, Forty-fifth report of Session 2022-23, HC 1254, April 2023.
7 Comptroller and Auditor General, *Tackling tax evasion in high street and online retail*, Session 2024-25, HC 229, National Audit Office, September 2024.

2.17 Inconsistent data formats and systems make it harder to use data to tackle fraud and error. Many of the counter-fraud teams we spoke to had to manually 'clean' data, correcting errors and making sure they are in a format and state they could use. This is a time-consuming and resource-heavy process. They also raised concerns about the interoperability of data, with the many different systems in use across government inhibiting data-sharing. GDS's blueprint for modern digital government sets out an ambition to improve contracting within the public sector and with the private sector so that data are more standardised and can be used across systems.

Challenge Seven: Managing the data-sharing process

2.18 Sharing data is crucial for effective data analytics to tackle fraud and error. For example, DWP uses HMRC income information to check a person's eligibility for Universal Credit, and to help decide the amount they should receive. Sharing data also helps bodies identify and protect against known fraudsters, or organised criminal groups (see case study 3, for example). The Information Commissioner's Office has recently produced guidance on how the UK General Data Protection Regulation and the Data Protection Act 2018 allow data-sharing to prevent, detect and investigate scams and frauds. The Digital Economy Act 2017 (DEA) provides one route for sharing personal data for defined purposes, which include the production of statistics, research purposes and to fight fraud (**Figure 6** on pages 35 and 36). The process had been used in 28 pilots related to fraud, of which four had transferred to business-as-usual, by June 2025 (Figure 4).

2.19 Public bodies continue to find it difficult and bureaucratic to share data to help tackle fraud, even though it is permitted under legislation. Officials told us that:

- **public bodies do not know what data can be shared, or the information that data protection officers need to agree a data-sharing arrangement:** There are significant data security and legal considerations to address before data can be shared. Counter-fraud teams sometimes have limited experience of data-sharing and told us they are unsure of the information they need to provide so that senior officials such as data protection officers will agree to arrangements, and that decisions often seemed to be based on the risk appetite of those senior officials. Counter-fraud teams also said the legislation was difficult to understand and navigate;

- **public bodies find it difficult to set up data-sharing under the DEA:** When senior officials agree in principle to sharing data, it can still be a lengthy process to set up the data-sharing agreements under the DEA process. Agreements can take months or even years to negotiate, partly so bodies can ensure the correct data security and protection protocols are in place. PSFA has an 'indicative timeline' which suggests that setting up a data-sharing agreement should take around 20 weeks, if stakeholders and the Secretariat 'act on a timely basis', but it does not have a formal monitoring process to check whether this is achieved; and

- **most data-sharing agreements are arrangements between two public bodies, when others could benefit from the same data:** For example, 23 of the 28 DEA pilots related to fraud included HMRC data. These were mostly set up through individual 'bilateral' agreements between HMRC and individual bodies. This puts resource pressures on a small number of data teams in government, and contrasts with the 'multilateral' data-sharing we have seen in the private sector. For example, many contribute to the Cifas National Fraud Database to help other participants identify fraud.

2.20 As more data are shared and systems linked, the risk increases that fraudsters penetrate one system to take advantage of another. We have already seen the mass attack of one government system designed to enable payments from another joined by data-sharing. Government has responded through established governance arrangements designed to provide assurance that the data met both parties' needs. But as government expands data-sharing across more departments, data governance and assurance arrangements will need to adapt accordingly.

Figure 6

Process to set up a counter-fraud data-sharing pilot under the Digital Economy Act 2017

Officials told us it can take a long time to set up and develop a data-sharing agreement though the Digital Economy Act 2017 (DEA) process

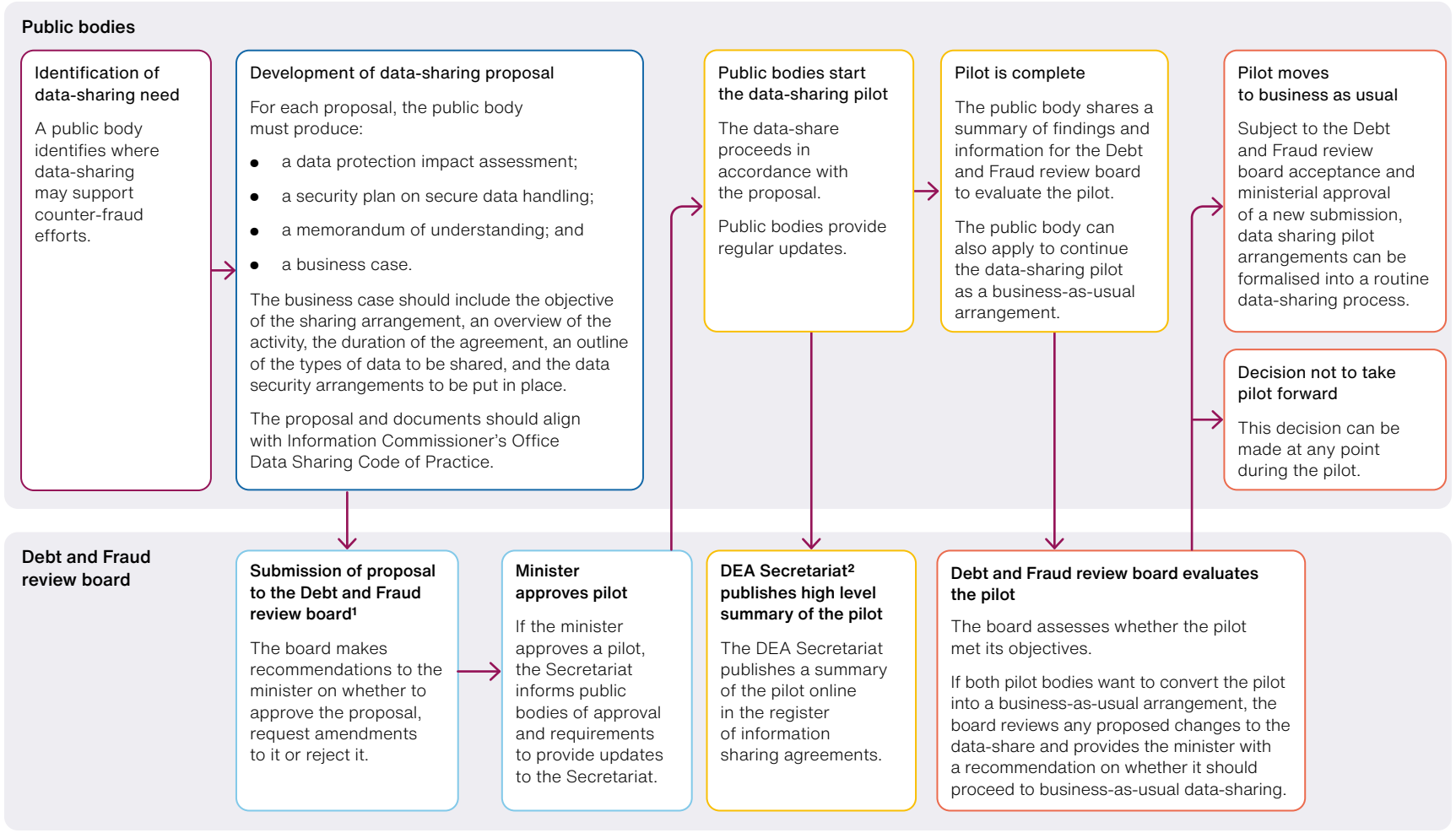


Figure 6 *continued*
Process to set up a counter-fraud data-sharing pilot under the Digital Economy Act 2017

Notes

1 The Debt and Fraud review board consists of central and local government officials who consider the appropriateness of data-sharing proposals and provide oversight of the pilots, with invited representatives including from public representative bodies and the Privacy and Consumer Advisory Group to capture the views of civil society. Representatives from the Information Commissioner's Office attend in an observer capacity.

2 The Secretariat to the Debt and Fraud review board is staffed by the Public Sector Fraud Authority.

3 Some pilots are only ever intended to be one-off data-sharing exercises. These pilots would not proceed to business-as-usual through the method shown above.

4 We have not reviewed how public bodies have used this process in practice.

Sources: National Audit Office analysis of *Digital Economy Act 2017*, part 5: Codes of Practice. Available at: www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice Accessed on 1 July 2025.

Challenge Eight: Putting in place the right skills

2.21 Effective use of data analytics to tackle fraud and error requires a blend of digital skills and fraud subject-matter expertise. We were told that developing data analytics tools to tackle fraud and error, including those with an AI element, requires mixed teams with skills in both data analytics and fraud and error. This is challenging because:

- **data analytics and digital teams are at a premium in public bodies and counter-fraud teams can struggle to access them:** The public sector is dependent on external digital expertise; according to GDS, the public secto spent £14.5 billion on digital contractors in 2023. GDS told us that, in April 2025, 5.5% of civil servants had expertise in digital and data. GDS is working to increase this proportion of digital, data and cyber professionals to 10%. We were told that it is difficult to build and retain teams with the right mix of skills; and
- **counter-fraud professionals often do not have digital skills, or experience of fraud prevention work:** Most fraud experts come from an investigation background and have limited data analytics skills.

2.22 Most of the successful data analytics projects we have seen have been developed by dedicated teams that bring these skills together. HMRC and DWP invest large amounts of resources into counter-fraud to build strong data analytics and digital counter-fraud expertise, as fraud and error represents a significant risk to their organisation. While we have also seen examples of smaller counter-fraud teams building successful data analytics tools, these teams often relied on the willingness of their organisation's digital team to lend support or on a standalone investment to upskill.

Challenge Nine: Optimising the staffing and algorithms to maximise the return

2.23 Fraud and error data analytics tools often require staff to review flagged payments, but departments have not always resourced this to the optimal level to maximise returns. We saw examples of public bodies applying 'risk scores' to help prioritise which transactions or payments their staff should investigate further. We have previously reported how staff shortages delay detection of overpayments from transactions flagged as risky, most notably in Carer's Allowance.[8] Increasing the use of data analytics to counter fraud and error may not result in staff reductions, even where it leads to savings through the greater prevention, detection and recovery of fraud and error. In the private sector, however, we saw organisations combine risk scoring with automated decision-making for low-risk transactions, to allow them to be processed faster and more cheaply.

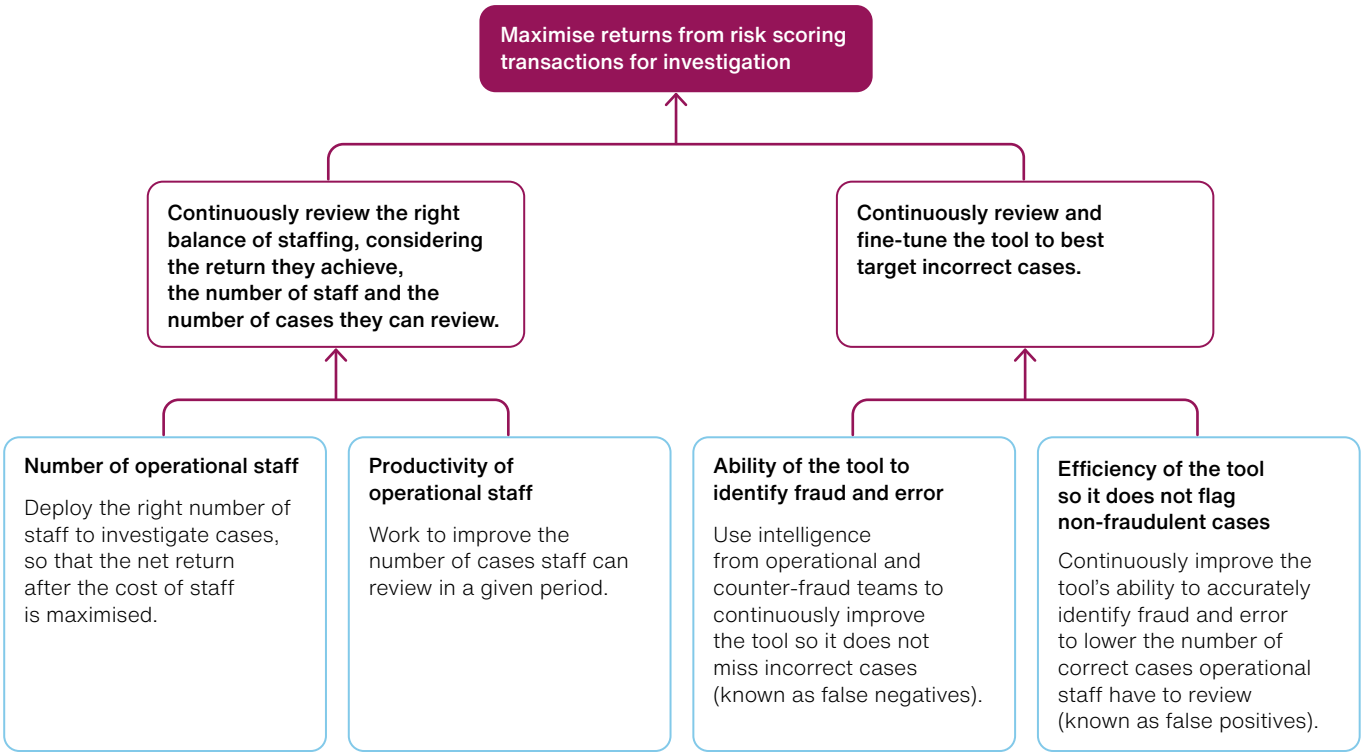
2.24 To maximise savings, public bodies also need to continually optimise algorithms to identify fraud and error, and investigate the right number of 'risky' cases. Without the right level of resourcing and effective prioritisation of cases to investigate, bodies will be unable to achieve the maximum return on investment into data analytics to fight fraud and error. To maximise return on investment, public bodies will need to optimise their staffing investment, staff productivity, output level of false positives and negatives relative to the number of transactions, and the average error rate and value of transactions investigated (see **Figure 7**).

8 Comptroller and Auditor General, *Investigation into overpayments of Carer's Allowance*, Session 2017-19, HC 2103, National Audit Office, April 2019 and Comptroller and Auditor General, *Carer's Allowance*, Session 2024-25, HC 377, National Audit Office, December 2024.

Figure 7

Maximising fraud and error savings through risk scoring

Optimising the number and productivity of staff, and fine-tuning the tool to best target incorrect cases, will maximise returns on investment for risk scoring



Notes

1 False positives are the cases flagged as potentially incorrect by the data analytics tool that are not actually incorrect.

2 False negatives are incorrect cases that were not flagged by the data analytics tool.

Source: National Audit Office analysis of government documents and previous National Audit Office work

Challenge Ten: Maintaining public trust while harnessing new capabilities

2.25 Public bodies must balance transparency about their use of data analytics with the risk of making it easier for fraudsters to take advantage. Various civil society bodies have raised concerns about the transparency and fairness of using data analytics to tackle fraud and error. Officials told us that meeting transparency requirements was sometimes difficult without revealing things that would make it easier for fraudsters to circumvent their controls. Most data analytics tools to fight fraud and error have not complied with the mandatory Algorithmic Transparency Recording Standard, designed to help public sector bodies publish information about the algorithmic tools they use when making decisions that affect members of the public. In addition, agreements set up and recorded through the Digital Economy Act 2017 have not always provided the information a reader would need to understand what data are being shared. We have not seen many examples of bodies reporting on the differential impact on customers of their data analytics. One exception is DWP which reports in its Annual Report and Accounts that its use of data analytics in Universal Credit Advances does not result in adverse impacts to customers, such as payment delays.[9]

2.26 Officials also raised concerns that a legal inhibition of profiling individuals was preventing them from making full use of data analytics to fight fraud. Private sector businesses use knowledge of previous fraudulent activity by individuals or entities that apply to use the businesses' services. Forensic auditors also told us they often look for links between payrolled individuals and suppliers using sophisticated network analysis. Cabinet Office told us that it was unable to use information about people's previous fraudulent behaviour to protect public funds, or use SNAP network analysis about officials' links to suppliers, because of text in the Local Audit and Accountability Act 2014, which states:

A data matching exercise may not be used to identify patterns and trends in an individual's characteristics or behaviour which suggest nothing more than the individual's potential to commit fraud in the future.[10]

9 Department for Work & Pensions, *Annual Report and Accounts 2023-24*, HC 62, July 2024, p. 112.
10 *Local Audit and Accountability Act* 2014, Schedule 9, 1(5), *Local Audit and Accountability Act 2014 (legislation.gov.uk)*, accessed 25 June 2025.

Appendix One

Our audit approach

Our scope

1 This report examines how well placed government is to seize the opportunity offered by old and new data analytics technologies to tackle fraud and error. We look at what government is already doing and set out the challenges. The report sets out:

- case studies of how the private sector and government are already using data analytics to tackle fraud and error; and
- lessons from these case studies and our discussions with those involved in implementing them about the strategic challenges.

We conducted fieldwork from February 2025 to May 2025.

Our evidence base

Scoping exercise

2 We emailed finance directors (FDs) of ministerial departments in February 2025. We asked for examples of data analytics being used in their departments and non-departmental public bodies within their departmental group. We asked the FDs to show us good practice examples of the use of data analytics to fight fraud and error, including both preventative and detective tools, and both innovative and well-established uses. We also asked them to nominate participants for our workshops and officials to interview with experience of using data analytics in their public body.

3 We used responses to this scoping exercise to select our case studies. To supplement the examples shared by FDs, we also reviewed recent Digital Economy Act 2017 pilots and Contracts Finder, government's public database of contracts between public bodies and the private sector.

4 This scoping exercise was non-exhaustive and led by the public bodies; they shared the examples and were not asked to share every tool they use. We interacted, through workshops or discussions with officials, with 24 of the 35 public bodies we initially asked.

Interviews with government officials

5 From January to May 2025, we spoke to public officials in the following bodies:

- Public Sector Fraud Authority (PSFA);
- Government Digital Service (GDS);
- Government Finance Function (GFF); and
- Crown Commercial Services (CCS).

6 We spoke to officials in our main audited bodies (PSFA, GDS and GFF) to understand their role in the use of data analytics to fight fraud and error. We also asked for any plans or strategies they had in place on the matter.

7 As the study progressed, we also interviewed officials from other bodies, like the Information Commissioner's Office, to understand the context of particular challenges and more detail on issues that arose in walkthroughs.

8 Interviews were conducted online.

Document review

9 We sent PSFA a document and meeting request log in early February 2025. This covered topics like PSFA's plans to improve data analytics to fight fraud, PSFA's understanding of barriers faced by government, and examples of good practice. We added to the document request log as the study progressed to make sure we had a broad understanding of the issues arising in walkthroughs and through our document review.

10 We reviewed documentation from PSFA from late February 2025 to May 2025. This provided us with insight into:

- government plans to develop (existing) data analytics tools to fight fraud and error;
- barriers faced in the public sector;
- evidence of central government bodies (PSFA, GDS, GFF) working together on data analytics to fight fraud; and
- lessons learned from the international arena and private sector.

11 Documents included roadmaps for the initiatives, tools and pilots run by PSFA, returns relating to fraud and error that were received by PSFA from other parts of government, and training packs that PSFA produced and provided to officials in government bodies.

Public sector case studies

12 We gained an understanding of some of the data analytics tools being used across government, informed by responses from FDs, Contracts Finder and the Digital Economy Act 2017 pilots. We then selected a number of public bodies and case studies to interview, aiming to ensure we had coverage of preventative and detective controls, well-established and pilot tools, and a range of different analytic types.

13 We conducted over 15 online walkthroughs with 12 public bodies, and decided to include 14 case studies from 10 public bodies in the report.

14 For each case study, we spoke to counter-fraud professionals and data scientists to understand how the tool worked and supported the public body's counter-fraud efforts. We asked the officials about how they had developed the tool, and the challenges they had faced. Although we interviewed relevant teams and conducted walkthroughs, we have not sought to verify the information provided by public bodies for our case studies. This includes savings amounts for the analytics tools, which were sometimes described to us as estimates.

15 While we aimed to cover a wide range of case studies, our known population of data analytics tools to fight fraud was not comprehensive. As such, our sample is not representative and there may be other data analytics tools being used to tackle fraud and error that are not included in this report.

Private sector case studies

16 We spoke to ten private sector stakeholders from across the banking, IT and insurance sectors in February and March 2025. Walkthroughs were conducted online. We used these walkthroughs to learn how data analytics are being used outside of government. We had multiple meetings with some stakeholders who were able to introduce us to private sector firms using their tools.

17 We drew on existing contacts we had as a team, and asked PSFA for contact details of firms that support government's use of data analytics to fight fraud. We explained to all private sector participants that we have no powers of access to their information and that they were sharing information with us on a voluntary basis. We also explained that we would not advocate for particular suppliers through our work.

18 During the walkthroughs, we also asked private sector organisations for insight into any challenges government might face when trying to use data analytics to fight fraud and error, or for any barriers the stakeholder had experienced when working with the public sector.

Workshops

19 We held two workshops in early March with officials who had experience of using data analytics to tackle fraud and error. These officials were nominated by their public body. The purpose of the workshops was to triangulate a long-list of challenges we had collated through review of documents, previous National Audit Office audits, and public and private sector case studies.

20 Twenty-six participants from 18 public bodies attended the workshops. We shared our long-list of challenges with attendees prior to the workshops and presented them briefly at the start of the workshops. We divided the workshops into two breakout group sessions and discussed the challenges faced in using data analytics to fight fraud and how to overcome them.

21 Participants in the workshops validated the long-list of challenges we had developed from our interviews and provided to them in advance. The counter-fraud professionals in attendance also added to and refined our list and told us how they would like to be supported by central government.

This report has been printed on Pro Digital Silk and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

National Audit Office

Design and Production by NAO Communications Team
DP Ref: 015415-001

£10.00
ISBN: 978-1-78604-627-7