National Audit Office

REPORT

Using data analytics to tackle fraud and error

Cross-government

SESSION 2024-25
9 JULY 2025
HC 988

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.