

Committee of Public Accounts

Government use of data analytics on error and fraud

Seventy-fifth Report of Session 2024–26

HC 891

Committee of Public Accounts

The Committee of Public Accounts is appointed by the House of Commons to examine “the accounts showing the appropriation of the sums granted by Parliament to meet the public expenditure, and of such other accounts laid before Parliament as the committee may think fit” (Standing Order No. 148)

Current membership

[Sir Geoffrey Clifton-Brown](#) (Conservative; North Cotswolds) (Chair)

[Mr Clive Betts](#) (Labour; Sheffield South East)

[Anna Dixon](#) (Labour; Shipley)

[Rachel Gilmour](#) (Liberal Democrat; Tiverton and Minehead)

[Sarah Green](#) (Liberal Democrat; Chesham and Amersham)

[Sarah Hall](#) (Labour; Warrington South)

[Lloyd Hatton](#) (Labour; South Dorset)

[Chris Kane](#) (Labour; Stirling and Strathallan)

[Rupert Lowe](#) (Restore Britain; Great Yarmouth)

[Catherine McKinnell](#) (Labour; Newcastle upon Tyne North)

[Sarah Olney](#) (Liberal Democrat; Richmond Park)

[Tristan Osborne](#) (Labour; Chatham and Aylesford)

[Michael Payne](#) (Labour; Gedling)

[Blake Stephenson](#) (Conservative; Mid Bedfordshire)

[Dan Tomlinson](#) (Labour; Chipping Barnet)

[Matt Turmaine](#) (Labour; Watford)

Powers

Powers of the Committee of Public Accounts are set out in House of Commons Standing Orders, principally in SO No. 148. These are available on the Internet via www.parliament.uk.

Publication

This Report, together with formal minutes relating to the Report, was Ordered by the House of Commons, on 23 March 2026, to be printed. It was published on 27 March 2026 by authority of the House of Commons.
© Parliamentary Copyright House of Commons 2026.

This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/copyright.

Committee reports are published on the Committee's website at www.parliament.uk/pac and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Public Accounts Committee, House of Commons, London SW1A 0AA. The telephone number for enquiries is 020 7219 8480 (strictly media enquiries only – contact us via our email for general enquiries); the Committee's email address is pubaccom@parliament.uk. You can follow the Committee on X (formerly Twitter) using CommonsPAC.

Contents

	Summary	1
	Conclusions and recommendations	3
1	Taking the opportunity to make fraud and error savings	8
	Introduction	8
	Potential savings from data analytics	9
	Government plans to achieve savings	10
2	Overcoming barriers to achieving savings	12
	Digital capability and leadership	12
	Sharing data effectively across government	14
3	Building public trust and optimising related legislation	16
	Transparency and maintaining public trust	16
	Legislative challenges	17
	Formal minutes	18
	Witnesses	20
	Published written evidence	21
	List of Reports from the Committee during the current Parliament	22

Summary

Fraud and error cost the taxpayer an estimated £55 to £81 billion a year, comprising £50 billion from unpaid tax or overpaid benefits and £5 billion to £31 billion from other areas of government. Government has been using data analytics to tackle fraud and error for years, but outside of the Department for Work and Pensions (DWP) and HM Revenue & Customs (HMRC), data analytics to tackle fraud are less developed and there has been a lack of ambition and activity to deploy this new technology. In January 2025, the Department for Science, Innovation and Technology (DSIT) estimated that using data analytics more widely across government could reduce fraud and error losses by up to £6 billion per year, but it has provided little detail on how and when this will be achieved.

Digital experts at the centre of government know the main barriers preventing the further roll-out of data analytics to bring fraud down: legacy IT systems; a lack of digital capability and leadership across government; and difficulty sharing data between government bodies. Additionally, legislation such as the Local Audit and Accountability Act, introduced in 2014, does not allow for profiling of individuals' behaviours, meaning that government cannot flag individuals who have committed fraud before as an indicator for future fraud detection work. This limits the use of some modern data analytics technology, and potentially stops government from achieving millions more in savings.

DSIT is the department responsible for coordinating digital transformation across government. It has decided to not go ahead with the appointment of a permanent secretary-level Government Chief Digital Officer, and instead the Government Digital Service (GDS) team will report into the DSIT Permanent Secretary. The new structure will include two new directors-general roles, one responsible for implementing the government's digital transformation agenda and the other responsible for digital products that the GDS builds and runs itself. However, DSIT has yet to demonstrate that it has sufficient influence across government to achieve the change it wants. More broadly, some parts of government lack senior leadership with strong digital skills, despite DSIT telling us that some key departments now have digitally skilled leaders at Board level.

While data analytics present a great opportunity to save money, government has not been transparent enough about how they are being used to maintain public trust. All government bodies are required to

publish information about the algorithms, artificial intelligence (AI) and machine learning they use on a central and publicly available register, but this register is not complete. Collectively, government is also not saying enough about its counter-fraud performance for the public to know their tax money is being spent wisely. The Public Sector Fraud Authority (PSFA) told us that it set and monitored fraud and error savings targets for all central government departments, but the targets and results for each department are not published.

Conclusions and recommendations

1. **Public bodies are not yet fully embracing the opportunity to save billions in fraud and error by using data analytics.** Losses through fraud and error cost the taxpayer an estimated £55 billion to £81 billion each year. While there are few direct comparators, the PSFA told us this represents a similar level of losses as in the US and EU. While the bulk of losses are in the tax and welfare systems, the rest of government still accounts for between £5 billion and £31 billion of fraud and error losses per year. DSIT knows that data analytics are vital to tackling this loss and has estimated they could save up to £6 billion per year. But we do not have confidence all public bodies share the ambition or are set up to achieve such savings, with only modest savings being achieved so far. The PSFA agrees annual targets for fraud and error savings with all central government departments and tracks how they perform against these, but these departmental targets and savings are not made public.

RECOMMENDATION

- a. HM Treasury should require public bodies to set out in their annual reports what they are doing to tackle fraud and error. This should include information about the targets public bodies agree with the Public Sector Fraud Authority, and how public bodies are performing against these targets.
- b. Public bodies should also be required to set out the type of counter-fraud activity they are conducting and how they intend to improve future performance.

2. **Government's digital and counter-fraud experts know what government needs to do to make fraud and error savings through data analytics, but do not have a robust plan to support public bodies to do so.** There are several barriers preventing the wider use of data analytics to fight fraud and error across government, including: the continued use of legacy systems; poor quality data; difficulties in sharing data; and a lack of digital skills in central government. However, while government knows what the barriers are, it lacks a detailed action plan to address them. DSIT published its delayed Roadmap for modern digital government in January 2026.

While this strategy sets out the government's ambition to embrace AI and replace legacy IT systems, it contains little detail on how and when this will be done and nothing on how this will help tackle fraud and error losses or what DSIT's responsibilities will be in this area.

RECOMMENDATION

The Government Digital Service, Public Sector Fraud Authority and Government Finance Function should set out how they will work together to deliver the reduction in fraud losses that data analytics can achieve, with clear targets and milestones. This should include how government intends to move from a system of detecting and recovering fraud, to one more focused on preventing fraud in the first place.

- 3. We are concerned that government has not built the digital capability or senior digital leadership it needs to achieve change and bring fraud savings from data analytics.** Digital transformation will require strong leadership. The government accepted the previous Committee's September 2023 recommendation that all departments should have a non-executive director with relevant digital, data and technology transformation expertise on their Boards. While DSIT assured us that this is now the case at several key departments, this ambition has not yet been achieved across government. GDS intends for at least 10% of the civil service to be digital, data and cyber professionals, but in April 2025 only 5.5% of the civil service met this criteria, and GDS is concerned that civil service pay rates make it difficult to retain digital leaders and achieve the upskilling it needs. We were also disappointed to hear that DSIT is not proceeding with the appointment of a permanent secretary-level Government Chief Digital Officer. It is instead choosing a structure where two directors-general will report into the DSIT permanent secretary, with responsibility for supporting digital transformation across government and the digital products GDS builds and runs. We believe this is a shortcoming, and that a Chief Digital Officer of appropriate seniority would give DSIT much greater clout across the whole of government to make the massive digital transformation that is necessary.

RECOMMENDATION

- a.** The Department for Science, Innovation and Technology should mandate that there are digitally skilled leaders at board level in all government departments, and all ALBs where technology plays a key part in their ations. It should also mandate the appointment of senior digital specialists in each department and ALB.

- b.** The Department for Science, Innovation and Technology should appoint a highly skilled Government Chief Digital Officer, at permanent secretary level, with the necessary authority and levers to bring about the digital transformation government wants to see.
- c.** The Department for Science, Innovation and Technology should clearly set out how it will meet the target of moving from 5.5% digitally trained civil servants to 10%, including the timetable for doing so. In reducing headcount in the civil service, it should concentrate on those functions that will be replaced by digital working.

- 4. Government is not doing enough to promote the effective sharing of data, which is stopping departments from maximising the savings they could make from data analytics.** Government bodies have legal frameworks through which to share data, such as those established by the Digital Economy Act 2017, but find it time-consuming and difficult to do in practice. The PSFA told us it is taking steps to make this process simpler and quicker. The PSFA also told us it is building a library of counter-fraud controls to encourage and enable better data sharing and to make it easier for government bodies to know what datasets and tools are already available. GDS said it was building a single data platform for use across government that will enable government bodies to find and use data assets. But government does not make full use of the other data-sharing tools available to it. For example, the National Fraud Initiative tool (NFI), which local authorities must use and through which they save millions of pounds by matching their own data with that of other local authorities, is not mandatory for central government. This means the NFI does not benefit from much of central government's data to help flag more potential fraud, and that central government itself does not realise some of the potential savings.

RECOMMENDATION

- a.** The Public Sector Fraud Authority should write to the Committee within 6 months to explain its progress in developing a library of counter-fraud controls. It should also set out its steps to identify and address issues with data sharing through the Digital Economy Act, to make this process simpler and quicker. This communication should include an evaluation of how its work has enabled greater sharing of data and greater use of data analytics.

- b.** In the Treasury Minute response to this report the Department for Science, Innovation and Technology should set out further information on the single data platform. This should include the timetable for completion and benefits, including in fraud and error, that the platform is expected to achieve.
- c.** HM Treasury, the Department for Science, Innovation and Technology and the Public Sector Fraud Authority should consider which elements of the National Fraud Initiative could be helpfully rolled out across central government, and mandate it accordingly.

- 5. Departments are not doing enough to be transparent or build public trust on the use of data analytics to tackle fraud.** In tackling fraud, government must balance maintaining public trust by being transparent about what it is doing, with not providing so much information that it helps fraudsters. We are concerned that government is not doing enough to assure the public that its use of data analytics is appropriate and does not disadvantage sections of the population. As an example, government bodies are required to disclose publicly any use of algorithms, AI and machine learning in decision making through the Algorithmic Transparency Recording Standard. DSIT told us that, while it believes it has captured most such uses, it knows that not all the expected cases have been recorded. As of February 2026, the Algorithmic Transparency Recording Standard repository held 11 records that mentioned ‘fraud’, and none of the good practice examples of data analytics case studies the NAO reported on were present on the register.

RECOMMENDATION

The Department for Science, Innovation and Technology should ensure that all government bodies comply with the Algorithmic Transparency Recording Standard so that the Hub captures all relevant uses of AI and machine learning. It should continuously monitor, update and ensure compliance with guidance around data analytics transparency to ensure that it maximises transparency without assisting fraudsters.

- 6. Current legislation limits government’s ability to deploy data analytics to tackle fraud and error.** Some existing legislation, such as the Digital Economy Act, support the use of data analytics to fight fraud and error by enabling data sharing across departments. However, there are also instances where legislation, written some time ago, does not fully support the effective deployment of modern data analytics techniques. For instance, the Local Audit and Accountability Act, introduced in 2014, does not allow for profiling of individuals’ behaviours. In practice, this means that it does not allow government to flag individuals who have committed fraud

before as an indicator for future fraud detection work, as would be done in other industries. Moreover, the data collected as part of the National Fraud Initiative, enabled by the Act, can only be retained for two years. This limits the ability to look at historical fraud trends and the range of data that can be used when trying to identify fraud.

RECOMMENDATION

- a.** The Public Sector Fraud Authority should review the legislation impacting its ability to implement fraud and error data analytics and communicate to Parliament where it believes additional powers or other changes to legislation would be helpful.
- b.** The Department for Science, Innovation and Technology and the Public Sector Fraud Authority should review the regulatory regime around government's fraud and error activities and communicate to Parliament where they believe additional powers or other changes to legislation would improve controls for specific fraud and error risks.

1 Taking the opportunity to make fraud and error savings

Introduction

1. On the basis of a report by the Comptroller and Auditor General, we took evidence from the Department for Science, Innovation and Technology (DSIT), the Public Sector Fraud Authority (PSFA), and the Government Finance Function (GFF) within HM Treasury.¹
2. 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. The NAO estimates that fraud and error cost the taxpayer between £55 billion and £81 billion in 2023–24.²
3. 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
4. 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

1 C&AG’s Report, Using data analytics to tackle fraud and error, [HC 988](#), 9 July 2025

2 C&AG’s Report, para 1

3 C&AG’s Report, para 2

services to local and central government, and encourages public bodies to make best use of data analytics to tackle fraud. The 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 and Technology.
- 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.⁴

Potential savings from data analytics

5. The PSFA told us that the £55 billion to £81 billion estimates for annual losses from fraud and error were comparable to levels calculated in the United States and European Union.⁵ It also stressed that these figures are gross and do not take into account the work that bodies like HM Revenue & Customs (HMRC) and the Department for Work and Pensions (DWP) do to recover these losses.⁶ According to PSFA and NAO estimates, around £40 billion of these losses come from tax (around £9 billion of these losses were actually detected, the remaining £31 billion is an estimate), £10 billion from welfare (around £2 billion of these losses were detected, the remaining £8 billion is an estimate), and the remainder (between £5 billion and £31 billion, with £1 billion detected) from other government activities.⁷
6. Counter-fraud experts, both within and outside of government, believe that data analytics need to be a key part of any plan to reduce fraud and error.⁸ The GDS has estimated that up to £6 billion of savings could be achieved by the effective use of data analytics.⁹ DSIT told us that this helped it present a strong case in the most recent spending review for

4 C&AG's Report, para 3

5 Q 4

6 Qq 4, 92

7 Q 4; NAO, [Good practice guide: Estimating and reporting fraud and error in annual reports and accounts](#), February 2025, p 7

8 C&AG's Report, para 1.2

9 C&AG's Report, para 6

investment in overcoming the barriers to their further roll-out.¹⁰ However, the NAO concluded that, to date, the savings achieved by government use of data analytics have been modest compared to their overall potential.¹¹

7. The PSFA told us that it now agrees annual targets for all government departments to reduce fraud error.¹² Its latest figures from 2023–24 suggest that working towards these targets is having a tangible impact in preventing and recovering fraud losses.¹³ Although DWP makes its own fraud reduction targets public, the bulk of departments agree targets internally with the PSFA and do not publish them.¹⁴ The PSFA also told us that these targets are set one year at a time – it does not have a longer-term target that it is aiming towards. Instead, it looks for departments to increase their impact in reducing fraud and error each year.¹⁵

Government plans to achieve savings

8. There are a number of issues that are undermining government’s efforts to use data analytics more widely to combat fraud and error. DSIT told us that that getting usable data can be difficult because they are held on legacy IT systems or because the data are not of good enough quality.¹⁶ The PSFA stated that government bodies find data-sharing, which underpins data analytics, difficult because different bodies use different data processes.¹⁷ Government has also acknowledged that some parts of the civil service do not have the level of digital skills required to use data analytics to their full potential.¹⁸
9. We recommended in March 2025 that government’s planned digital and AI roadmap should be underpinned by a implementation plan with clear accountabilities, delivery milestones, and metrics to allow progress to be tracked.¹⁹ The NAO report echoed this, further recommending that the PSFA publish a plan setting out how it will support public bodies across government to make the best use of data analytics to tackle fraud and error.²⁰ DSIT published its Roadmap for modern digital government in January 2026, some six months later than was originally intended and

10 Q 26

11 C&AG’s Report, para 1.4

12 Q 5

13 Q 5

14 Qq 8-10

15 Qq 13-14

16 Q 26

17 Q 35

18 Q 85

19 Committee of Public Accounts, Use of AI in Government, Eighteenth report of session 2024–25, [HC 356](#), March 2025, recommendation 6a

20 C&AG’s Report, Recommendation 1

around a week after our evidence session for this inquiry.²¹ While the strategy does mention some of the key issues such as enabling better use of AI and replacing outdated IT systems, it contains few concrete milestones to measure progress against and has little to say about using technology to combat fraud and error or what DSIT's responsibility will be in this area.

21 HMG, [A roadmap for modern digital government](#), January 2026

2 Overcoming barriers to achieving savings

Digital capability and leadership

10. The previous Committee recommended in September 2023 that all Departments should appoint at least one non-executive director with relevant digital, data and technology transformation expertise to their Board.²² This recommendation is reflected in the Government's new Roadmap for modern digital government, which sets an expectation that by December 2026 "Central and local government will be expected to have a digital leader on their executive committee and a digital non-executive director on their board."²³ DSIT told us that the 'big digital delivery departments', for the most part, already have digital officers at senior levels in their executive team and on their non-executive boards, but that this is not the case across all government bodies.²⁴
11. The Cabinet Office told us in March 2025 that, to achieve annual savings of up to £500 million by reducing the need for digital consultants, it was aiming for 10% of civil servants to have digital expertise.²⁵ Only 5.5% of the civil service met this criteria in April 2025, though DSIT told us that some government departments had already met this 10% target and that others are progressing towards it.²⁶ It also told us that while there are schemes, such as apprenticeships, aimed at developing government's digital capability, it faces challenges in recruiting and retaining at senior digital roles because of the wide pay differentials between the public and private sectors. DSIT told us that there is a degree of pay flexibility in making senior appointments and that it makes the case for these to be used, working with HM Treasury.²⁷ We reported in December 2025 that the

22 Committee of Public Accounts, Digital transformation in government: addressing the barriers to efficiency, Seventieth report of session 2022–23. [HC 1229](#), 13 September 2023, Recommendation 3b

23 HMG, [A roadmap for modern digital government](#), January 2026, 'Elevating digital leadership across government' section

24 Q 87

25 [Letter from Cabinet Office](#), 24 March 2025 (letter incorrectly dated 24 March 2024)

26 Q 85

27 Q 41

digital pay framework has been revalorised, but that it still falls short of industry rates in London and the South East, and this affects recruitment and retention.²⁸

12. At present much work on sharing best practice and increasing digital and counter-fraud capability across government is carried on through networks and communities of practice, though not all colleagues who might benefit from these sessions are in attendance.²⁹ The PSFA told us that it works with DSIT and the community of practice to produce guidance and training to reflect the nature of counter-fraud work, and building standards and qualifications for people working in fraud.³⁰ The Government Counter-Fraud Function also circulates guidance, including guidance on data analytics pilot schemes to combat fraud that it produced in conjunction with counter-fraud colleagues from Australia.³¹
13. As confirmed in January 2025's Blueprint for modern digital government policy paper, cross-government digital leadership now resides with DSIT.³² The blueprint included a plan to raise the status of the Government Chief Digital Officer to second permanent secretary-level. DSIT told us that it has now replaced the Government Chief Digital Officer, who was responsible for all the digital work within the GDS, with two new directors general posts. One of these is the director-general for digital products who is responsible for the various products that GDS builds and runs itself; the other is the director-general for digital transformation who is responsible for the architecture that supports other government departments to deliver their digital programmes (including progressing the digital profession, improving data and promoting the use of AI).³³ Neither role of director-general for digital transformation or director-general for digital products has been filled permanently, although interim appointments were made to both posts in January 2026.³⁴

28 Committee of Public Accounts, Government services: identifying costs, Fifty-Eighth report of session 2024–26. [HC 1421](#), 12 December 2025, Conclusion 5

29 Qq 45–46

30 Qq 33 and 45–46

31 Q 46

32 DSIT, A blueprint for modern digital government, [CP 1252](#), January 2025

33 Q 86

34 [Emily Middleton](#) has been appointed as interim DG for digital and [Christine Bellamy](#) has been appointed as interim DG for digital products

Sharing data effectively across government

14. The Digital Economy Act 2017 established a process through which government bodies can agree arrangements to share data with one another. The NAO reported that, as of July 2025, there had been 28 data-sharing pilot agreements set up through this process to tackle fraud, although only four had become business-as-usual processes.³⁵ The NAO noted that government bodies found it difficult and time-consuming to conclude these data-sharing agreements. The PSFA had an ‘indicative timeline’ which suggested that setting up a data-sharing agreement should take around 20 weeks, but the NAO found that the process could take months or even years to negotiate and that the PSFA does not have a formal monitoring process to check whether this is achieved.³⁶ The PSFA told us that, in response to these findings, it had produced a number of standard templates which it hopes will make the process quicker and simpler.³⁷ It also noted that projects initiated through the Digital Economy Act had achieved benefits in excess of £200 million in reducing fraud.³⁸
15. The National Fraud initiative (NFI) is a tool created in 1996 that brings data together from across the public sector to help bodies look for fraud and, to a lesser extent, for error. The NFI was originally focused on local authorities, who are required to use it. But the PSFA told us it is now increasingly used by central government bodies as well.³⁹ Thirty-six central government bodies (including arm’s-length bodies) took part in the most recent NFI exercise in 2024–25, an increase from 22 bodies in the previous iteration.⁴⁰ The PSFA told us that there is more that could be done with the NFI and there are parts of it that it would encourage greater use of.⁴¹ It explained to us that central government bodies are not mandated to use the NFI because the original legislation was targeted at local government and has not since been amended.⁴² The Treasury told us that there may be an option to mandate central government bodies to feed data into the NFI even if they were not going to use it themselves. However, it also said that government has chosen not to mandate central government bodies to participate, as not all would have useful data.⁴³ In written evidence provided after the session, the PSFA provided a preliminary estimate that making

35 C&AG’s Report, para 2.5

36 C&AG’s report, para 2.19

37 Qq 36-37 and 57

38 Q 82

39 Qq 48-49

40 C&AG’s Report, Figure 5

41 Q 48

42 Q 52

43 Q 53

the NFI mandatory for central government departments, and amending legislation to allow more data matching activities, could realistically save between £120 million and £150 million per two-year National Fraud Initiative cycle. Even under the PSFA's most conservative modelling, it still projected a net uplift of approximately £60 million per two-year cycle.⁴⁴

- 16.** The NAO report noted that, at present, there is no available library of counter-fraud tools and examples for government bodies to refer to.⁴⁵ It recommended that the PSFA should maintain a library of digital counter-fraud control that public bodies can use to find ways to address their fraud risks.⁴⁶ The PSFA told us that it felt that this was a useful recommendation and is taking the project forward.⁴⁷ DSIT told us that it was in the process of creating a single register of data assets that will ultimately underpin a platform that enables data sharing across government. Its intention is that this will highlight instances of successful data sharing and encourage government bodies to learn from them.⁴⁸

44 [Letter from the Public Sector Fraud Authority](#), 12 March 2026

45 C&AG's Report, para 2.6

46 C&AG's Report, recommendation 2

47 Q 83

48 Qq 27 and 43-44

3 Building public trust and optimising related legislation

Transparency and maintaining public trust

17. The PSFA told us that it is important to use data to fight fraud, and to maintain public trust that government bodies are holding their data in accordance with Parliament's intentions.⁴⁹ The C&AG told us that, while transparency in government operations was a positive thing, when dealing with counter-fraud measures it is important to not provide so much information that it helps fraudsters to circumvent controls.⁵⁰ The PSFA outlined that its current approach is to disclose what data analytics are being used to fight fraud and to let the public know how their data will be used, but not to make public the various checks it performs on the data.⁵¹
18. To ensure transparency, government bodies are required to disclose the use of algorithms, AI and machine learning through the Algorithmic Transparency Recording Standard (ATRS) hub.⁵² As at February 2026 the hub, which requires records of any such items used in decision making, recorded 110 being used in central government. Of these records, 11 mention 'fraud'.⁵³ None of the items the NAO report listed as good practice examples were recorded in the hub. DSIT reported that departments find the process challenging as they do not want to provide information that might help fraudsters, and it provides guidance on this subject.⁵⁴ DSIT acknowledged that the ATRS hub was not a complete record, but told us that it was confident it had recorded the majority of cases.⁵⁵
19. The NAO noted that DWP provided an example of good practice in transparency by setting out in its annual report and accounts how it ensures that its use of data analytics does not result in adverse impacts

49 Q 37

50 Q 25

51 Q 74

52 Qq 69-70

53 Government Digital Service, [Algorithmic Transparency Recording Standard Hub](#), accessed 3 February 2026

54 Qq 71-72

55 Q 71

to customers.⁵⁶ When we considered DWP's 2023–24 accounts, we were concerned that the department's use of data analytics and machine learning might have a detrimental impact on customers. DWP assured us that it had conducted a fairness impact assessment, but that it could not publish the results as they could assist fraudsters.⁵⁷

Legislative challenges

20. The PSFA told us that current legislation, for example the Digital Economy Act 2017 mentioned previously, is an essential foundation for the use of data analytics to fight fraud and error. That Act provided a mechanism which enabled government bodies to share certain datasets, allowing for greater use of data analytics.⁵⁸
21. However, the PSFA also told us that there are instances where legislation, written some time ago, does not fully support the effective deployment of modern data analytics techniques. For example, the Local Audit and Accountability Act 2014 does not allow for profiling of individuals' behaviours. Which means in practice that data collected under that Act can be used to look for or prevent fraud, but it cannot be used for ongoing live fraud investigations. It also does not allow the data to be used to flag individuals who have previously committed fraud to inform future counter-fraud work. The PSFA told us that, in other industries, it would be standard practice to use evidence that someone has committed fraud as an indicator that they may do so again.⁵⁹
22. Legislation also requires that data collected as part of the National Fraud Initiative, enabled by the Local Audit and Accountability Act, can only be retained for the two years – the duration of each biennial exercise. The PSFA told us that this data would be useful to inform counter-fraud work if it was retained for longer. This is common practice in other industries where they use historical data on fraud to identify trends and train models to understand what to look for. We note that it is common practice elsewhere for records to be retained for longer. For instance, HMRC requires companies to retain records for six years.⁶⁰

56 C&AG's Report, para 2.25

57 HC Committee of Public Accounts, DWP Customer Service and Accounts 2023–24, Sixth report of session 2024–25, [HC 354](#), 31 January 2025, para 7

58 Q 92

59 Q 92

60 Qq 92 and 96

Formal minutes

Monday 23 March 2026

Members present

Sir Geoffrey Clifton-Brown, in the Chair

Mr Clive Betts

Anna Dixon

Rachel Gilmour

Sarah Green

Chris Kane

Catherine McKinnell

Blake Stephenson

Matt Turmaine

Government use of data analytics on error and fraud

Draft Report (*Government use of data analytics on error and fraud*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 22 read and agreed to.

Summary agreed to.

Conclusions and recommendations agreed to.

Resolved, That the Report be the Seventy-fifth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available
(Standing Order No. 134).

Adjournment

Adjourned till Thursday 26 March at 9.30 a.m.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the [inquiry publications page](#) of the Committee's website.

Thursday 15 January 2026

Mark Cheeseman OBE, Chief Executive, Public Sector Fraud Authority;
Emran Mian, Permanent Secretary, Department of Science Innovation
and Technology; **Conrad Smewing**, Director General, Public Spending and
Joint-Head of the Government Finance Function, HM Treasury [Q1-97](#)

Published written evidence

The following written evidence was received and can be viewed on the [inquiry publications page](#) of the Committee's website.

GDA numbers are generated by the evidence processing system and so may not be complete.

1	Alamsetti, Mr Suman	GDA0008
2	Amnesty International UK	GDA0018
3	Ballis, Dr Antonis (Senior Lecturer in Finance and FRG Member, Aston University); and Kassem, Dr Rasha (Senior Lecturer in Accounting and Finance & Leader of the Fraud Research Group (FRG), Aston University)	GDA0012
4	Buziuk, Hleb	GDA0001
5	Heydari, Dr Mohammad	GDA0009
6	Holland, Stuart	GDA0003
7	Kaczmarek, Professor Sylvester	GDA0004
8	Mandal, Dr Anandadeep	GDA0005
9	Open Rights Group	GDA0016
10	Padmanabhan, Dr Deepak	GDA0006
11	Krupiy, Tetyana (Lecturer, Newcastle University)	GDA0010
12	Warsame, Mo	GDA0002
13	medConfidential	GDA0007

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the [publications page](#) of the Committee's website.

Session 2024–26

Number	Title	Reference
74th	Environmental regulation	HC 1687
73rd	Financial sustainability of adult hospices in England	HC 1236
72nd	BBC World Service	HC 1299
71st	Government's use of external consultants	HC 1521
70th	Home-to-school transport	HC 1238
69th	Whole of Government Accounts 2023-24	HC 1243
68th	Excess Votes 2024-25	HC 1711
67th	NS&I's transformation programme	HC 1237
66th	Tackling fraud and error in benefit expenditure 2024-25	HC 1231
65th	Efficiency and resilience of the Probation Service	HC 1235
64th	Costs of clinical negligence	HC 1234
63rd	Increasing police productivity	HC 1239
62nd	Faulty energy efficiency installations	HC 1229
61st	Financial sustainability of children's care homes	HC 1233
60th	DWP follow-up: Autumn 2025	HC 1447
59th	Ministry of Justice follow-up: Autumn 2025	HC 1240
58th	Government services: Identifying costs	HC 1421
57th	Government services: Generating income	HC 890
56th	BBC Accounts and Trust Statement 2024–25	HC 1230
55th	Reducing NHS waiting times for elective care	HC 820
54th	Afghanistan Response Route	HC 1391

Number	Title	Reference
53rd	Cost of maintaining the FCDO's overseas estate	HC 884
52nd	Resilience to threats from animal disease	HC 885
51st	The UK's F-35 stealth fighter capability	HC 1232
50th	Local bus services in England	HC 892
49th	Administration of the Civil Service Pension Scheme	HC 888
48th	Smarter delivery of public services	HC 889
47th	First Annual Report of the Chair of the Committee of Public Accounts	HC 1300
46th	Improving local areas through developer funding	HC 886
45th	Improving family court services for children	HC 883
44th	Governance and decision-making on major projects	HC 642
43rd	MoD's oversight of Reserve Forces' and Cadets' Associations	HC 893
42nd	Water sector regulation	HC 824
41st	UK Research and Innovation	HC 826
40th	Collecting the right tax from wealthy individuals	HC 827
39th	Government's use of private finance for infrastructure	HC 821
38th	Increasing teacher numbers: Secondary and further education	HC 825
37th	Immigration: Skilled worker visas	HC 819
36th	Jobcentres	HC 823
35th	Introducing T Levels	HC 822
34th	Department for Business and Trade Annual Report and Accounts 2023-24	HC 818
33rd	Supporting the UK's priority industry sectors	HC 1070
32nd	The Future of the Equipment Plan	HC 716
31st	Local Government Financial Sustainability	HC 647
30th	Antimicrobial resistance: addressing the risks	HC 646
29th	Condition of Government property	HC 641
28th	Decommissioning Sellafield	HC 363
27th	Government's relationship with digital technology suppliers	HC 640
26th	Tackling Violence against Women and Girls	HC 644
25th	DHSC Annual Report and Accounts 2023-24	HC 639
24th	Government cyber resilience	HC 643
23rd	The cost of the tax system	HC 645
22nd	Government's support for biomass	HC 715

Number	Title	Reference
21st	Fixing NHS Dentistry	HC 648
20th	DCMS management of COVID-19 loans	HC 364
19th	Energy Bills Support	HC 511
18th	Use of AI in Government	HC 356
17th	The Remediation of Dangerous Cladding	HC 362
16th	Whole of Government Accounts 2022-23	HC 367
15th	Prison estate capacity	HC 366
14th	Public charge points for electric vehicles	HC 512
13th	Improving educational outcomes for disadvantaged children	HC 365
12th	Crown Court backlogs	HC 348
11th	Excess votes 2023-24	HC 719
10th	HS2: Update following the Northern leg cancellation	HC 357
9th	Tax evasion in the retail sector	HC 355
8th	Carbon Capture, Usage and Storage	HC 351
7th	Asylum accommodation: Home Office acquisition of former HMP Northeye	HC 361
6th	DWP Customer Service and Accounts 2023-24	HC 354
5th	NHS financial sustainability	HC 350
4th	Tackling homelessness	HC 352
3rd	HMRC Customer Service and Accounts	HC 347
2nd	Condition and maintenance of Local Roads in England	HC 349
1st	Support for children and young people with special educational needs	HC 353