Bank of England PRA

FCA FINANCIAL CONDUCT AUTHORITY

Dame Meg Hillier, MP
Chair, Treasury Select Committee
House of Commons
London
SW1A 0AA

Andrew Bailey
Governor
Bank of England

Nikhil Rathi
Chief Executive
Financial Conduct Authority

4 November 2026

Dear Dame Meg,

Critical Third Parties regime and Google Cloud service disruptions

Thank you for your letter of 20 October 2026 concerning the disruption to Google Cloud EMEA Limited ('Google'). In line with the joint oversight arrangements for Critical Third Parties (CTPs), the Bank of England, Prudential Regulation Authority and Financial Conduct Authority (together, the authorities) are responding jointly.

This letter provides the authorities' initial response, based on the information currently available. A number of the committee's questions require further analysis and reflection, including through the post-incident review which is currently underway. We will provide a fuller response by 20 January 2027, drawing on that work and providing further information to answer the committee's questions in full.

The Authorities' operational resilience framework and Critical Third Parties regime

Addressing non-financial resilience is an ever wider and more complex task, not least as the frequency and materiality of operational and cyber incidents grows. We recognise that these incidents can cause disruption for businesses and consumers. The authorities' operational resilience framework seeks to reduce the likelihood and severity of disruption, while recognising that not every operational incident can be prevented. Its purpose is to protect financial stability by ensuring that individual firms, CTPs and the financial system as a whole can minimise the impact of disruption, maintain the delivery of critical services within agreed tolerances and recover effectively.

The occurrence of disruption does not, by itself, determine whether the framework has operated effectively. That assessment depends on the causes and impact of the incident, the adequacy of the preparations made and the effectiveness of the response and recovery.

The authorities have taken a number of steps in recent years to strengthen the operational resilience of the UK financial sector. We have emphasised the importance of firms obtaining sufficient assurance that their material third parties can respond to and recover from severe disruption. Where sufficient assurance cannot be obtained firms should strengthen their own contingency arrangements and consider practicable alternative provision. The CTP regime forms an important part of that framework. Its objective is to manage risks to the stability of, or confidence in, the UK financial system that may arise from a failure of, or disruption to, services provided by a CTP to the financial sector.

The CTP regime complements, rather than replaces, the responsibilities of regulated firms and financial market infrastructures (FMIs). Firms and FMIs remain responsible for their own operational resilience and for managing the risks arising from their reliance on third parties, while recognising that the delivery of important services may depend on a small number of critical external providers. CTPs must manage and identify risks to the systemic third-party services they provide, and maintain open, timely communication with the regulators and the firms that rely on them, particularly during major incidents. As disruption cannot be eliminated in its entirety, the framework for firms, FMIs and CTPs focuses on limiting the disruption's impact and supporting effective recovery.

HM Treasury decides whether to designate a third party as a CTP, generally following a recommendation from the authorities. HM Treasury designated Google Cloud EMEA Limited ('Google') as a CTP on 13 July 2026. Designation recognises that certain

services provided by Google to the UK financial sector meet the statutory criteria for systemic third-party services. These are services whose failure or disruption, could threaten the stability of, or confidence in, the UK financial system.

As with any serious incident, an interruption to services provided by a designated CTP requires careful examination to establish all the facts. After the initial response phase described below, we are now conducting our post-incident review. This involves assessing both the causes of this incident and how effectively Google and affected firms were able to limit the impact of the interruption, to restore services and so support the stability of, or confidence in, the UK financial system. The review will take into account further information provided by firms as they conduct their own post-incident reviews.

The Google outage and its impact

Google experienced a complete power loss in a data centre facility in its europe-west2-b zone, beginning at 07:00 BST on Tuesday 20 October 2026. Service provision from that zone was affected for approximately seven hours. Google reported that the incident had been mitigated for most customers by 15:03 BST.

On the morning of Tuesday 20 October, we became aware of the disruption at 09:09 BST through affected firms, not initially through a notification from Google itself; subsequently Google provided information during the incident alongside updates through its public service-health channels.

The outage disrupted a range of Google Cloud Platform services and affected a wide range of Google’s customers, including firms in the UK financial sector. Firms use Google cloud services in different ways and with different configurations. The effects were therefore not uniform, and some firms experienced more significant disruption than others. Reported effects included disruption to customer-facing banking and payments services and to internal operational and risk management systems, including systems supporting asset-management and trading. The incident also affected unregulated third-party service providers that provide outsourced services to regulated firms, creating indirect effects through firms’ supply chains.

Although the underlying data centre issue was resolved during the afternoon and customer firms were able to reconnect to Google cloud services, some firms required additional time to restore their own services and return to normal operations.

Affected firms activated contingency arrangements, limiting disruption to the services they provide. Recovery across the sector was generally swift and by the end of the day almost all business-as-usual operations had resumed. The incident caused material disruption for some consumers while affected firms were unable to provide certain

services. These disruptions were resolved as firms reconnected to Google and no material ongoing effects on consumers have been identified. There were no identified implications for market integrity or wider financial stability during or following the incident.

On 22 October, Google published a preliminary root cause analysis, later followed by a more detailed analysis on 27 October. Google attributed the incident to an external electrical outage caused by an underground cable fault outside the data centre facility supporting its europe-west2-b zone. The data centre's back-up generator failed to receive the signal required to start and the available battery reserves were subsequently depleted, resulting in the loss of power to infrastructure supporting the zone. Google's investigation and post-incident review and lessons learned are continuing.

The authorities' response

As soon as the authorities became aware of the disruption at Google, we invoked our established cross-authority incident-response arrangements. These arrangements were used to coordinate engagement across the financial regulators, wider authorities and with industry, share information and maintain a system-wide view of the incident and its effects.

The financial authorities' Joint Oversight Team responsible for Google engaged with Google throughout the duration of the incident. Relevant supervisory teams at the PRA and FCA engaged with affected regulated firms where appropriate (no Bank-supervised FMIs were affected). Information from these sources was brought together through the authorities' cross-sector arrangements.

Alongside this engagement, we kept the need for a wider cross authority response under review through the Authorities Response Framework (ARF) which enables the financial authorities to coordinate their response to potentially systemic operational incidents or threats affecting the sector. The Bank, PRA, FCA, HM Treasury, the National Cyber Security Centre and the Payment Systems Regulator considered the information provided by Google, the impact on affected firms and the wider sector, the effectiveness of contingency arrangements, and whether further escalation was required. During this incident the ARF protocol enabled relevant authorities to maintain a shared view of developments, impacts and risks and to keep the need for further cross-authority action under review.

We also gathered sector wide intelligence through established sector coordination arrangements. The Financial Sector Cyber Collaboration Centre monitored for any indication of a cyber cause, while the UK Finance Business and Operational Continuity Committee engaged with its members to assess the wider effects of the incident. No

indication of malicious activity was identified, and further escalation was not considered necessary.

Follow up and next steps

We are engaging with Google and affected firms through the relevant post-incident review processes. We will also review the operation of our own arrangements.

That work will inform our fuller response to the Treasury Select Committee, including further information on the incident, its impact and the lessons identified.

We hope that this initial response is helpful. We will write again by 20 January 2027.

Yours sincerely,





Andrew Bailey
Governor
Bank of England

Nikhil Rathi
Chief Executive
Financial Conduct Authority