

Dame Meg Hillier
Chair of the Treasury Committee
House of Commons
Palace of Westminster
Westminster
LONDON
SW1A 0AA

10 June 2025

Dear Dame Meg,

Unauthorised Access to HMRC Online Tax Accounts

Thank you for inviting me to give oral evidence to the Treasury Committee on Wednesday 4 June. I am writing to provide further detail on the PAYE fraud security incident, which was raised during the hearing. I can also offer a private briefing if the Committee would value an in-confidence security briefing to explore the issue further. I have also received your letter today, 10 June, and will respond to this in due course.

HMRC operates one of the UK's largest and most complex IT estates. Like many tax authorities worldwide, our systems are subjected to constant attack. HMRC analyses approximately 200 billion events across systems monthly, proactively blocking around 1.5 billion suspicious activities. In total, we prevented £1.9 billion in revenue loss in 2023 to 2024 by stopping fraudulent registrations and repayment claims by criminals.

To further strengthen HMRC's resilience to identity-related fraud, HMRC is developing a Fraud Prevention Centre (FPC), which is a multi-functional team led by HMRC's Security department, focusing on the continued protection, detection and response to identity-related security issues. Additionally, the FPC will deliver enhanced support direct to customers, managing fraud in line with industry best practice.

As I said at our evidence session, HMRC commenced criminal investigations last year. Having identified misuse of accounts, HMRC took action to protect customer data and secure compromised accounts, which included:

- identifying and locking down affected online tax accounts
- deleting login credentials to prevent further unauthorised access
- removing incorrect information added to tax records
- checking no other customer details were changed.

HMRC's Audit and Risk Committee was briefed last autumn; and throughout, HMRC has liaised with the Information Commissioner's Office, whilst actively pursuing the criminal groups, careful to protect confidential live investigations.

Having undertaken complex checks and remediation, the team has concluded that approximately 100,000 customers (around 0.22% of our total customer base) had potentially been impacted. From 4 June to 25 June, we are sending letters to these customers to provide guidance and advice on next steps, having also briefed key stakeholders including professional bodies representing tax agents so they could provide support to any affected customers, and supporting affected customers who contacted HMRC directly.

We recognise this incident may be of concern, especially to those customers who may have been affected. The Committee should be reassured that HMRC has put comprehensive support in place including a dedicated GOV.UK page and telephone helpline, and provided reassurance that no customers have experienced, or will experience, any financial loss in respect of their tax affairs as a result of this incident. We stand ready to respond to customer needs as they arise.

Regarding losses to the Exchequer, I would like to correct the oral evidence, as the estimated PAYE revenue losses are £49 million, not £47 million as we stated during the hearing. The normal route for notifying losses to Parliament is through the Annual Report and Accounts where HMRC includes individual incidents exceeding £10 million in the Trust Statement and exceeding £300,000 in the Resource Accounts in line with *Managing Public Money* requirements. I understand that under *Managing Public Money*, losses of this value would not be considered material. I will, nonetheless, report the issue in our forthcoming Annual Report, due to be published next month.

I welcome the Committee's interest in matters related to security and would like to be clear this is the very highest priority for HMRC. We take the security of our customers' data extremely seriously and HMRC will continue to enhance our security measures and capabilities to tackle the continuous, evolving security challenges faced by all large institutions. Given the sensitive nature of the issue, my team and I would be available to attend a private briefing if the Committee would value an in-confidence security briefing and like to explore the issue further.

I am also writing to the Chair of the Committee of Public Accounts.

Best wishes,



John-Paul Marks
CHIEF EXECUTIVE AND FIRST PERMANENT SECRETARY