Inland Revenue
Te Tari Taake

26OIA2341

24 June 2026

[redacted]

Dear [redacted]

Thank you for your request made under the Official Information Act 1982 (OIA), received on 26 May 2026. You provided copies of two responses to OIA requests on the topic of unauthorised access to taxpayer information along with these follow up questions:

1. *How many individual taxpayers had their records accessed across the 107 formal investigations and types of taxpayer information were accessed? eg financial returns/employer data/child support/student loans/KiwiSaver.*
2. *Did any cases involve downloading, printing, photographing, emailing, or externally sharing taxpayer information?*
3. *Did any investigations find evidence information was used for personal, financial, retaliatory, or criminal purposes?*
4. *Why were only 107 of 351 suspected cases escalated into formal employment investigations? Did any of the staff involved hold senior or managerial roles?*
5. *Does IRD consider 72 dismissals over six years to indicate a systemic integrity problem?*
6. *Did IRD seek advice from the Privacy Commissioner on whether notification was required?*
7. *Why were the taxpayers whose records were breached not informed? How does IRD define "serious harm" in the context of privacy breaches?*
8. *How many of the 72 staff members were referred to Police over taxpayer data access?*
9. *The OIA response says: "One risk report was expanded in 2023 in response to findings from a prior breach." How many additional cases of unauthorised access were identified as a result of the expanded risk report that were not previously being detected?*

On 27 May 2026, Inland Revenue responded to parts 5 through 8 of your request via email, I have included that information in this response for completeness. The information you have requested for parts 1 through 4 and 9 is provided below.

Background

Inland Revenue has a zero-tolerance approach to integrity issues. Inland Revenue makes it very clear what is expected of staff through its training, policies, and Code of Conduct and has confidential channels to make it easy for people to report suspected misconduct, fraud, or wrongdoing.

All suspected misconduct, fraud, or wrongdoing must be reported immediately to Inland Revenue's Integrity & Conduct Unit. The Unit is independent, and its mandate is to act on any wrongdoing at any level within Inland Revenue. The Integrity & Conduct Unit authorises and oversees all staff related investigations.

Monitoring in place

Alongside the ability for staff and the public to report suspected wrongdoing (including unauthorised access), Inland Revenue also proactively monitors access to its systems to help prevent and detect misuse of systems and information. The tools and resources used to detect unauthorised access continue to evolve as technology improves and to adapt to emerging patterns of behaviour. Following an investigation, there may be instances where additional checks and monitoring are implemented.

Where unauthorised access is alleged or detected, action is taken quickly. Every allegation received by the integrity team is looked into and those where the circumstances raise concerns over the legitimacy of the access are investigated further.

From our recent OIA reply, there were 351 suspected cases between 2019-2024. 107 were escalated into formal employment investigations. As a result of these investigations, 72 staff were dismissed. In the 244 cases that were not escalated there was no evidence found that unauthorised access had occurred.

Consequences for unauthorised access

Where it is determined that unauthorised access has occurred, disciplinary action including considering dismissal, is taken. Inland Revenue has strict statutory obligations regarding the confidentiality of customer information. The dismissals reflect the strictness of those obligations, and the rigorous and evolving nature of our monitoring systems.

We recognise that the public's reasonable expectation is that Inland Revenue will maintain high standards around confidentiality. Inland Revenue processes millions of tax returns annually and deals with millions of NZ taxpayers. In that context, the level of dismissals reflects that we take our confidentiality obligations seriously, and that our detection methods work.

Inland Revenue is responsible for prosecuting matters under the legislation it administers, including breaches of confidentiality requirements. However, Inland Revenue will involve the Police if other criminal matters are found through the course of an investigation.

Informing affected customers

Customers and the Privacy Commissioner are required to be informed of notifiable privacy breaches. Under section 112 of the Privacy Act 2020, a notifiable privacy breach means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals, or is likely to do so.

Section 113 of the Privacy Act then sets out factors that should be considered when assessing the likelihood of serious harm being caused by a privacy breach. Inland Revenue uses these factors to determine whether affected customers are notified. We did not seek advice from the Privacy Commissioner on whether notification was required.

Question 1: How many taxpayers had their records accessed across the 107 formal investigations and types of taxpayer information accessed.

Across the 107 formal employment investigations relating to unauthorised access to taxpayer information, a total of 480 individual taxpayer records were accessed.

These investigations involved staff accessing taxpayer information relating to addresses, bank accounts, correspondence, file notes, and account information for tax and social policy products administered by Inland Revenue (e.g. income tax, student loans, Working for Families tax credits).

Question 2: Did any cases involve downloading, printing, photographing, emailing, or externally sharing taxpayer information?

Of the 107 formal employment investigations, 10 cases involved the extraction of information from Inland Revenue systems. Of these, eight cases involved sending information to the customer themselves. One involved sending information to the customer's tax agent, and one involved sending information to Charities Services.

Question 3: Did any investigations find evidence information was used for personal, financial, retaliatory, or criminal purposes?

Of the 107 formal employment investigations, there were 19 cases where it was found that the information accessed was used in some way to benefit the staff member or the customer.

Administrative or service benefits occurred when the unauthorised access to information resulted in the bypassing of Inland Revenue's established channels or processing standards (for example, skipping the queue), or receiving a service outside of Inland Revenue's standard operating methods (for example, having an address updated without going through the normal process). All 19 instances of unauthorised access involved administrative and / or service benefits.

Question 4: Why were only 107 of the 351 suspected cases escalated into formal employment investigations? Did any of the staff involved hold senior or managerial roles?

As outlined in the *Monitoring in place* section of this response, the remaining 244 cases were not escalated to formal investigations as there was no evidence that unauthorised access had occurred.

Of the 107 formal employment investigations, one involved an Inland Revenue staff member who held a Team Leader position. No cases involved senior staff.

Question 9: The OIA response says: "One risk report was expanded in 2023 in response to findings from a prior breach." How many additional cases of unauthorised access were identified as a result of the expanded risk report that were not previously being detected?

Of the 107 cases of unauthorised access mentioned in our previous OIA response, 13 were identified as a direct result of the new detection methods in our expanded risk report.

Cases of unauthorised access have become much easier to identify as a result of Inland Revenue's constantly evolving safeguards and new technology enabled by our Business Transformation programme, in which we upgraded our computer system to one with more capability for detecting improper use. These new detection methods have allowed Inland Revenue's Integrity & Conduct Unit to analyse patterns of behaviour and retrieve targeted information from our old systems. In some cases, this would uncover prior unauthorised access to information that would not have otherwise been detected in the old system.

Right of review

If you disagree with my decision on your OIA request, you have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the OIA. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Publishing of OIA response

We intend to publish our response to your request on Inland Revenue's website (ird.govt.nz) as this information may be of interest to other members of the public. This letter, with your personal details removed, may be published in its entirety. Publishing responses increases the availability of information to the public and is consistent with the OIA's purpose of enabling more effective participation in the making and administration of laws and policies and promoting the accountability of officials.

Thank you again for your request.

Yours sincerely

Chris Linton
Domain Lead – Integrity & Conduct