Privacy Commissioner
Te Mana Mātāpono Matatapu

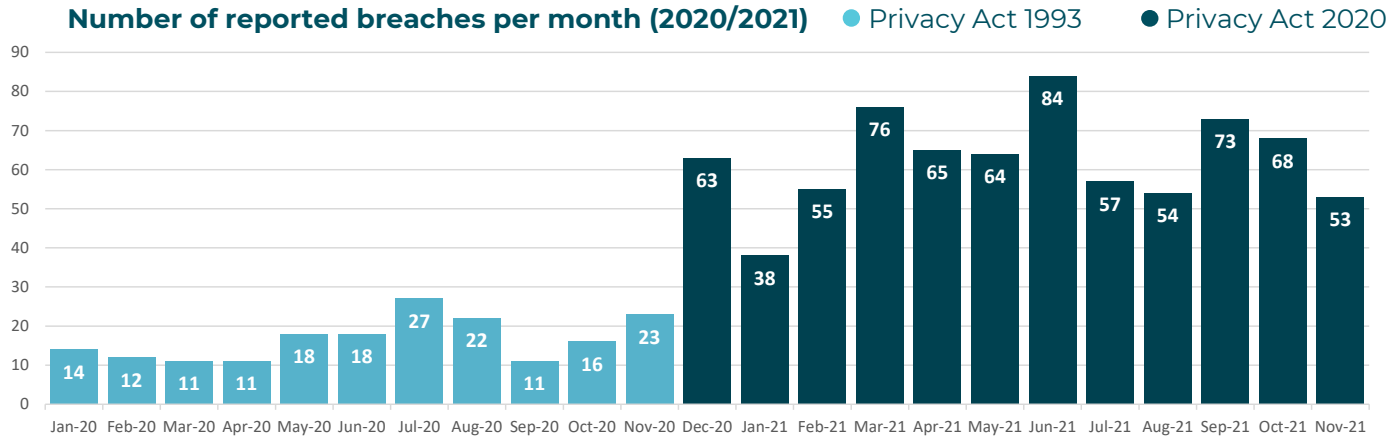
# Mandatory privacy breach reporting one year on

**1 December 2020 - 30 November 2021**

## Privacy breaches reported to us have increased significantly since reporting became mandatory

From 1 December 2020 it became mandatory to notify the Office of the Privacy Commissioner of privacy breaches that have caused, or have the potential to cause, serious harm to people. Between 1 December 2020 and 30 November 2021, we received a total of 750 privacy breach notifications, nearly four times as many as between 1 December 2019 and 30 November 2020. You can use our NotifyUs tool to help you determine whether you need to notify us of your breach and to complete the notification if you do.

**Number of reported breaches per month (2020/2021)**




## Our NotifyUs tool can help you decide whether your breach needs to be reported to us

A third of all privacy breaches reported between 1 December 2020 and 30 November 2021 met the threshold for serious harm. If you are unsure if your breach meets the threshold for reporting to us, you can use our anonymous self-assessment tool to help you decide. Every case is different and it is not always clear cut whether the breach is serious or not. We encourage organisations to err on the side of caution and report to us if you think the breach *could* be serious. If in doubt, report your privacy breach.


**33%** of all reported breaches met the serious harm threshold.

## Privacy breaches cause real harm to people

Privacy breaches can cause many types of harm to people. Between 1 December 2020 and 30 November 2021, 36% of serious breaches reported to us have involved emotional harm.

Emotional harm is the result of a privacy breach which has caused significant humiliation, significant loss of dignity or significant injury to an individual's feelings.

| Type of harm | |
|---|---|
| Emotional harm | 36.4 % |
| Reputational harm | 14.4 % |
| Identity theft | 13.3 % |
| Financial harm | 11.1 % |
| Threats of harm | 5.0 % |
| Employment harm | 5.0 % |
| Loss of information | 4.4 % |
| Discriminatory harm | 3.9 % |
| Loss of opportunity | 3.5 % |
| Physical harm | 3.1 % |

Example

*An email containing detailed health information about a group of patients was intended to be sent internally to the staff of a medical provider. A typing error in the 'TO' field resulted in a member of the public receiving these patients' medical records. Having their sensitive personal information exposed in this way caused considerable emotional harm to a number of these patients.*

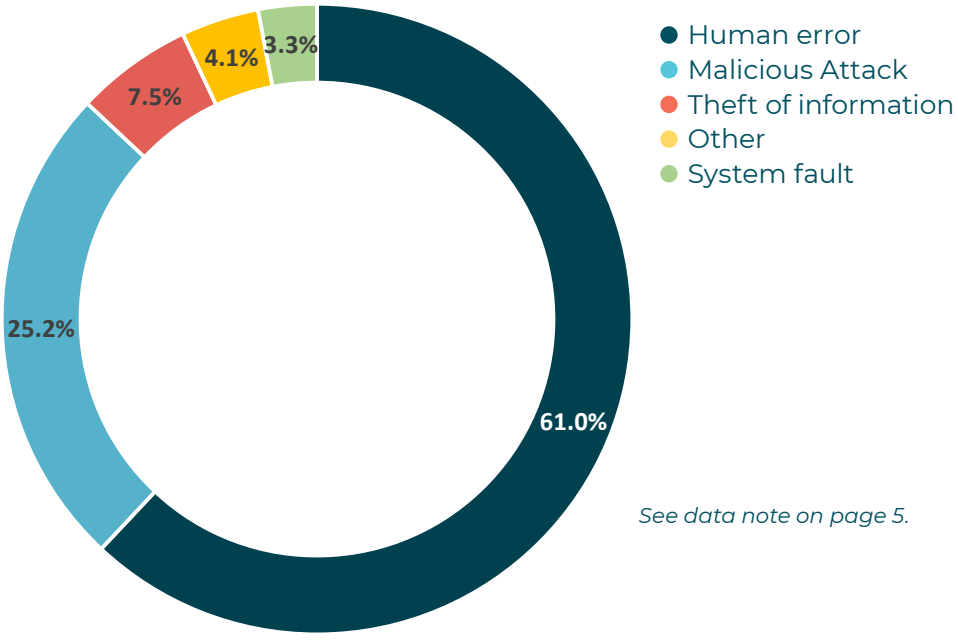
*Note: Types of harm are not mutually exclusive. Hence, one privacy breach often involves more than one type of harm.*

## The majority of serious breaches reported are the result of human error

The most common type of human error causing privacy breaches is email error. Email error accounts for over a quarter of all reported serious privacy breaches. Other types of human error include accidental disclosure of sensitive personal information, data entry errors, confidentiality breaches, redaction errors, postal and courier errors.

Email error is easy to prevent through good systems and processes. Be careful when including personal information in emails, double check attachments, have a send delay and use BCC when sending to multiple recipients. A warning was given to one agency for having multiple privacy breaches caused by email error and we are prepared to take further enforcement action if agencies repeatedly experience privacy breaches caused by email error.

### Causes of privacy breaches




*See data note on page 5.*

## Privacy breaches can occur in any sector

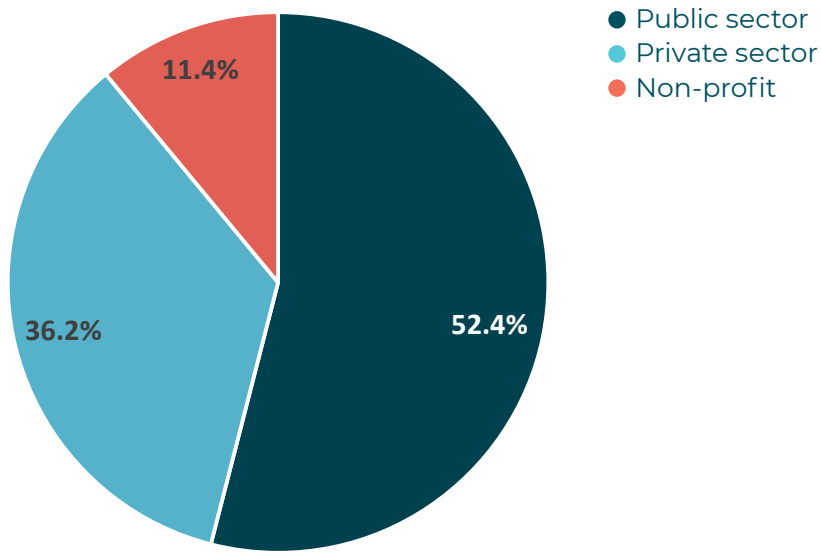
We see privacy breaches reported to us from the public, private and not for profit sectors as well as a wide range of industries. Almost all organisations hold some form of New Zealanders' personal information and they need to ensure it is well protected.

Health care and social assistance is by far the industry classification which reports the highest number of privacy breaches.

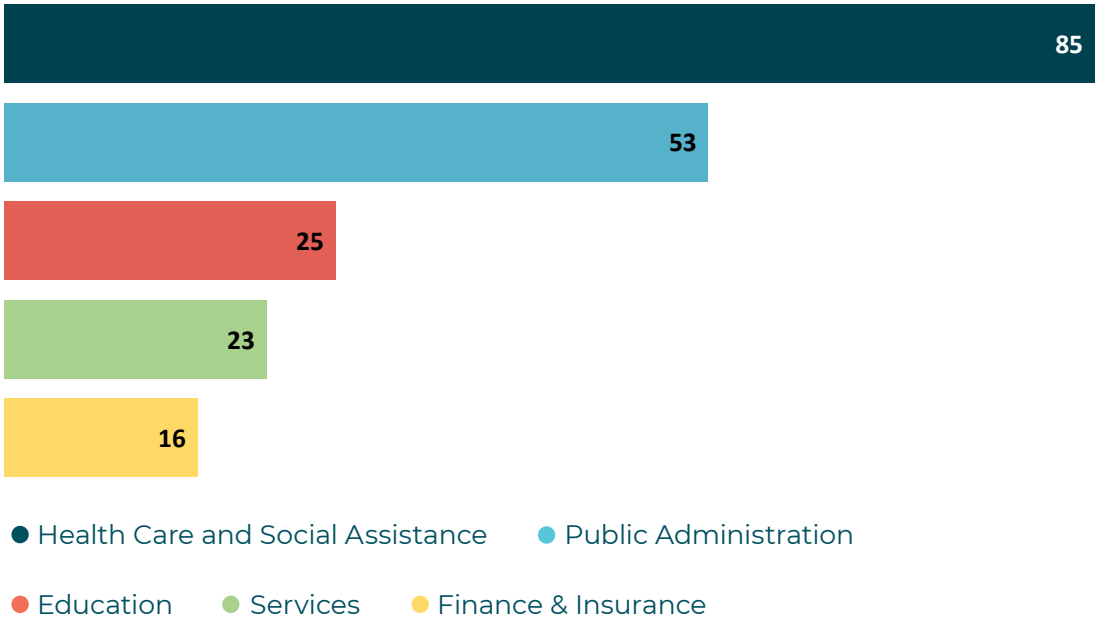
A high number of notifications from one sector or industry doesn't necessarily indicate poor privacy practice - it may mean that these sectors are more aware of their obligation to report privacy breaches.

Good privacy practice means detecting and reporting serious privacy breaches to us, as well as putting systems in place to ensure they don't happen again.

### Serious privacy breach notifications by sector




### Top five industries reporting serious privacy breaches

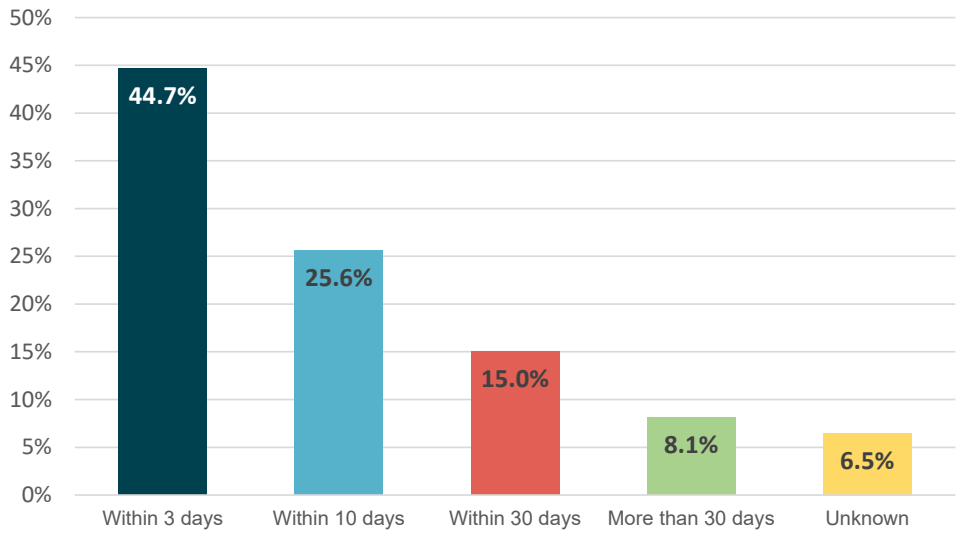


## We expect you to notify us of a serious breach within 72 hours of identifying it

In June this year, we set out our expectation around the timeliness of privacy breach notification clear. A notifiable breach should be reported to us no later than 72 hours after an agency has become aware of it. Currently, less than half of all serious breach notifications are being made within the expected timeframe.

You should not wait until you have all the details of the privacy breach, our NotifyUs tool allows you to update the notification at a later stage, as more information becomes available. The sooner we know about a breach, the sooner we can support you to reduce potential harm to affected individuals.

### Timeliness of breach reporting to OPC




*Note: 'Unknown' refers to cases when the date of identification of the breach is not known.*

## Have affected individuals been notified by the time OPC is informed of the privacy breach?

Only 61% of agencies had contacted the affected individuals by the time they reported the breach to us. We understand that it will often take longer to work through notifying impacted individuals than the expected 72 hours to NotifyUs. However, there are limited grounds for not telling people that their personal information has been involved in a privacy breach.

These exceptions for not notifying affected people include:

- It would likely be harmful to their health
- They are under the age of 16 and it would likely not be in their interest
- It would be harmful to NZ's security or international relations
- It would likely be harmful to the maintenance of the law
- It would likely endanger someone's safety
- It would likely reveal a trade secret


**61%** of affected individuals had been notified by the time the Office was informed of the privacy breach

- Had been notified
- Had not been notified

## About our data

This report captures notifications made under the NotifyUs scheme for the period from 1 December 2020 to 30 November 2021. NotifyUs statistics are current as of 18 January 2022. However, a number of recent notifications included in these statistics may still be under assessment and their categorisation may be subject to change after publication of this report.

The figures in the report's tables and graphs do not always add up to 100% due to the rounding up or down of the percentages for each category.

### Cause

The cause of any given breach is based on information provided by the reporting agency. Where more than one cause has been identified or is possible, the dominant or most likely source has been selected. Cause of breach categories are: Human error, Malicious attack, Theft, System error, Other.

- *Human error*

An unintended action by an individual directly resulting in a privacy breach, e.g. inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.

- *Malicious attack*

A malicious attack deliberately crafted to exploit known vulnerabilities for financial or other gain, e.g. ransomware or phishing attacks.

- *Theft of information*

This category refers to both theft of physical documents and identity theft.

- *System fault*

A business or technology process error not caused by direct human error.

Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
T +64 4 474 7590 Fax +64 4 474 7595
E enquiries@privacy.org.nz
privacy.org.nz