

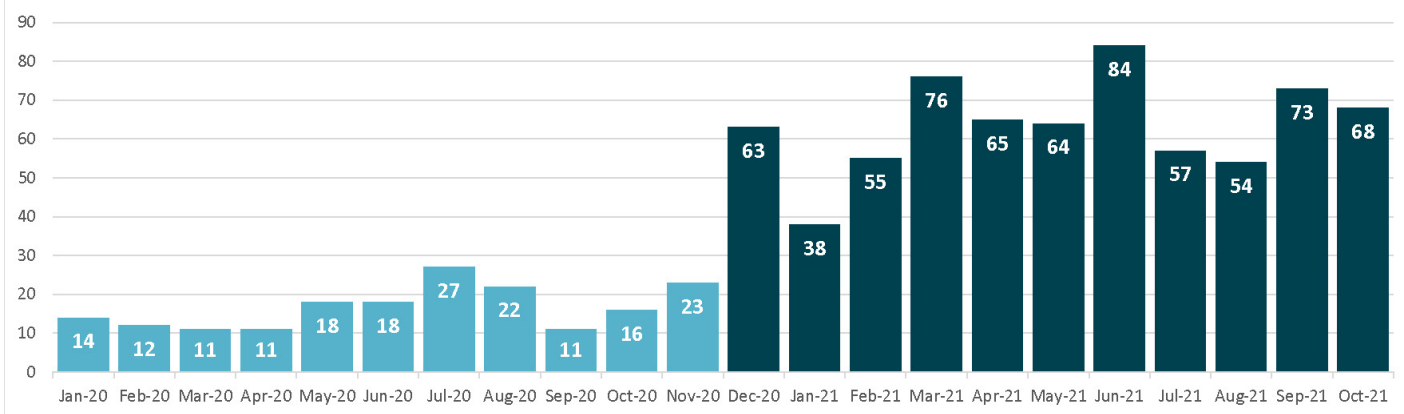
Mandatory privacy breach reporting one year on

1 December 2020 - 31 October 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 31 October 2021, we received a total of 697 privacy breach notifications, nearly four times as many as between 1 December 2019 and 31 October 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) ● Privacy Act 1993 ● Privacy Act 2020



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 31 October 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 31 October 2021, 35% 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	35 %
Reputational harm	14 %
Identity theft	13 %
Financial harm	11 %
Threats of harm	5 %
Employment harm	5 %
Loss of information	4 %
Discriminatory harm	4 %
Loss of opportunity	3 %
Physical harm	3 %

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.

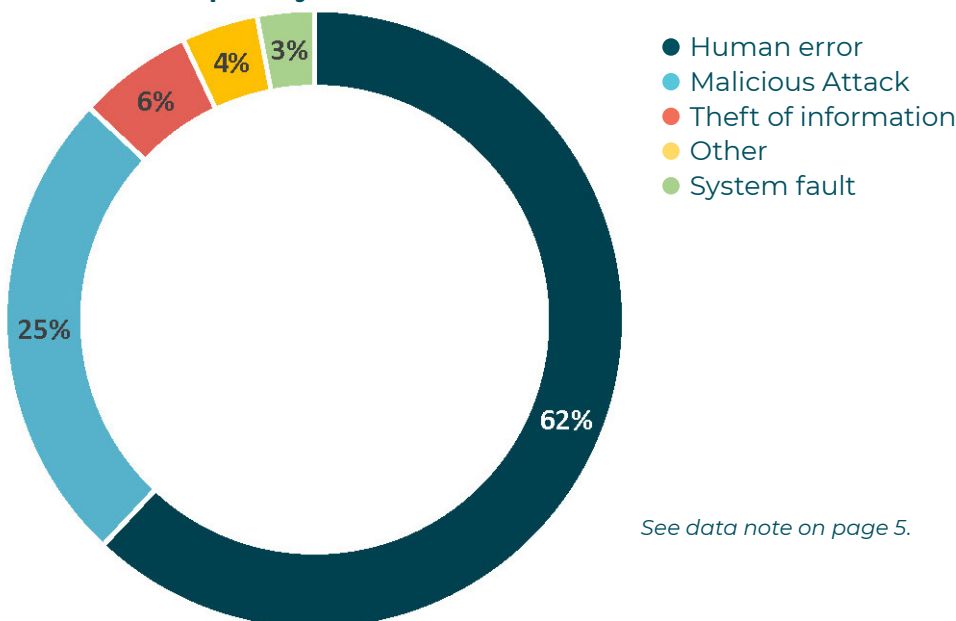
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category. Types of harm are not mutually exclusive. Hence, one privacy breach often involves more than one type of harm.

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

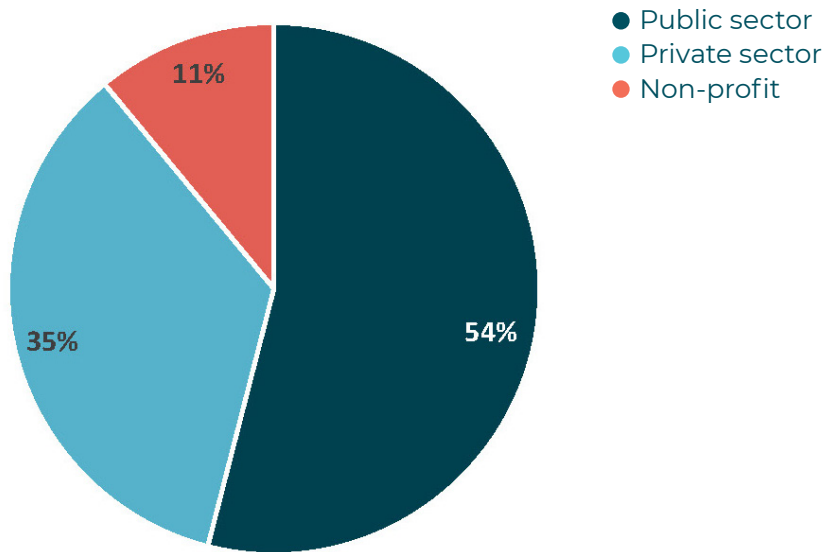
We see privacy breaches reported to us from the public, private and not for profit sectors as well as a wide range of industries. Almost all organisations hold some form of New Zealanders' personal information and they need to ensure it is well protected.

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

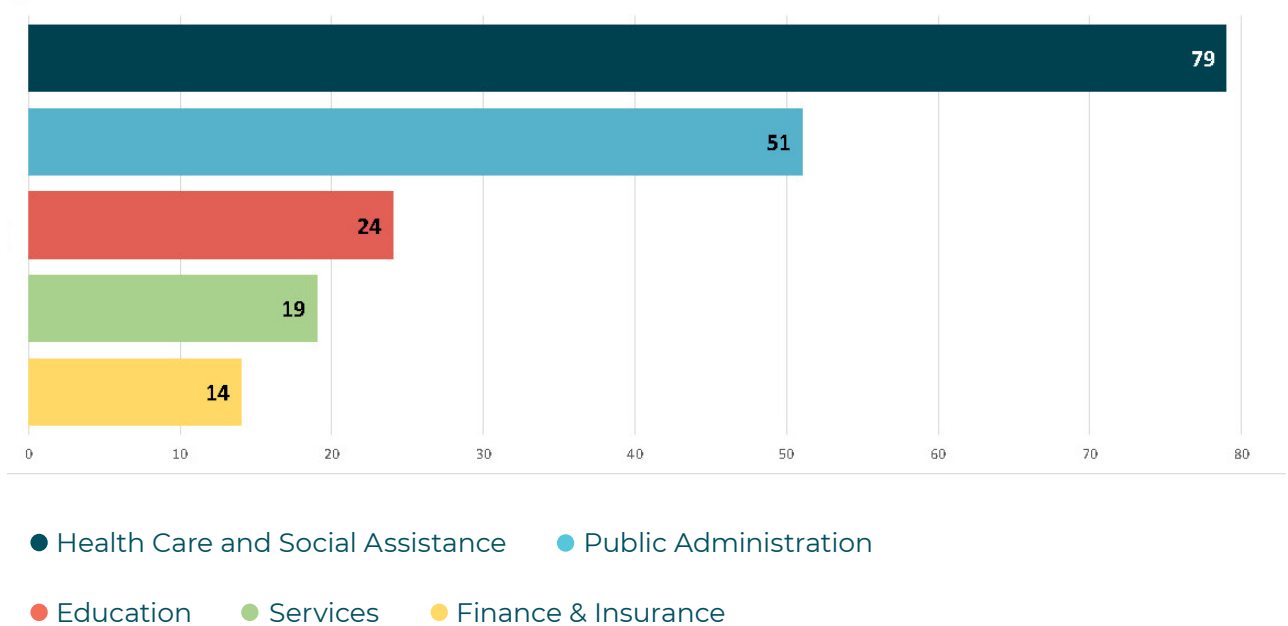
A high number of notifications from one sector or industry doesn't necessarily indicate poor privacy practice - it may mean that these sectors are more aware of their obligation to report privacy breaches.

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

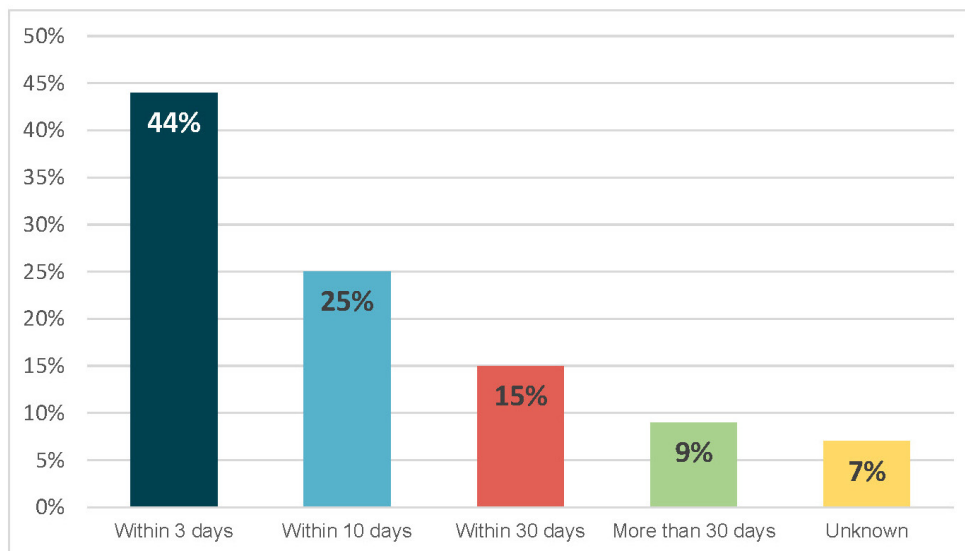


We expect you to notify us of a serious breach within 72 hours of identifying it

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 31 October 2021. NotifyUs statistics are current as of 16 November 2021. 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.

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*

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.



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



Appendix B: Financials for period ending 31 December 2021

Statement of Comprehensive Income For the 6 Months to 31 December 2021

Prev. Year YTD Actual \$000		Dec 2021 YTD Actual \$000	Dec 21 YTD Budget \$000	YTD Var \$000	YTD Var %	Year-End Outlook \$000	Year-End SPE Forecast \$000
	Revenue						
4,850	Revenue from Crown	3,696	3,696	-	-	7,392	7,392
131	Other Income	273	103	170	165	361	191
1	Interest	1	1	-	-	2	2
4,982	Total revenue	3,970	3,800	170	5	7,755	7,586
	Expenditure						
495	Marketing	22	73	(51)	(70)	133	184
-	Audit Fees	-	-	-	-	34	34
112	Depreciation	143	134	9	7	319	310
202	Rental	213	215	(2)	1	430	431
858	Operating	508	670	(162)	24	1,389	1,342
1,882	Staff Costs	2,556	2,638	(82)	3	4,933	5,226
3,549	Total expenditure	3,442	3,730	(288)	8	7,238	7,527
1,433	Net surplus / (deficit)	528	70	458	654	517	59

Statement of Financial Position As at 31 December 2021

	Dec 2021 Actual \$000	Dec 2021 Budget \$000	YTD Var \$000	Year-End Outlook \$000	Year-End SPE Forecast \$000
ASSETS					
Current Assets					
Cash & Cash Equivalent	1,644	940	704	1,590	1,057
Debtors and Other Receivables	59	30	29	80	35
Prepayments	77	100	(23)	100	100
Total Current Assets	1,780	1,070	710	1,770	1,192
Current Liabilities					
Creditors and other payables	140	160	(20)	131	160
Employee Entitlements	247	260	(13)	247	260
Total Current Liabilities	387	420	(33)	378	420
Working Capital	1,393	650	743	1,392	772
Non-Current Assets					
Property, Plant and Equipment	366	288	78	297	197
Intangible Assets	346	641	295	425	596
Capital Work in Progress	23	-	23	-	-
Total Non-Current Assets	735	929	(194)	722	793
Non-current Liabilities	19	20	(1)	16	17
Net Assets	2,109	1,559	550	2,098	1,548
Public Equity					
Opening Balance	1,581	1,489	92	1,581	1,489
Accumulated Surplus	528	70	548	517	59

	Dec 2021	Dec 2021	Year-End	Year-End
	Actual	Budget	YTD	SPE
	\$000	\$000	Var	Forecast
	\$000	\$000	\$000	\$000
	Outlook			
	\$000			
Total Public Equity	2,109	1,559	550	1,548

**Statement of Cash Flows
As at 31 December 2021**

	Dec 2021	Dec 2021	Year-End	Year-End
	Actual	Budget	Outlook	SPE
	\$000	\$000	\$000	Forecast
	\$000	\$000	\$000	\$000
Cash Flows from Operating Activities				
<i>Cash was Provided from:</i>				
Government Grant	3,696	3,696	7,392	7,392
Other Income	266	103	357	192
Interest	1	1	2	2
	3,963	3,800	7,751	7,586
<i>Cash was Applied to:</i>				
Payments to Suppliers	801	952	2,014	1,987
Payments to Employees	2,709	2,642	5,085	5,230
Payments of GST	(29)	(48)	5	(42)
	3,481	3,546	7,104	7,175
Net Cash Flow applied to Operating Activities	482	254	647	411
Cash Flows from Investment Activities				
Cash was applied to				
Purchase of Fixed Assets	111	290	330	330
<i>Net Cash flows applied to Investing Activities</i>	111	290	330	330
Cash was Provided from:				
Sale of Fixed Assets	1	-	1	-
Net Cash Flow from Investment Activities	(110)	(290)	(329)	(330)
Net Increase/(Decrease) in Cash Held	372	(36)	318	81
Cash brought forward	1,272	976	1,272	976
Closing cash carried forward	1,644	940	1,590	1,057
Cash made up of:				
Cash on hand	-	-	-	-
National Bank - Cheque	141	140	140	257
National Bank - Deposit	1,503	800	1,450	800
	1,644	940	1,590	1,057

Appendix C: Performance against Statements of Service Performance - Year to Date

Output 1 – Strategy and Insights

Measure	Achieved As at 31 Dec	Expectation As at 31 Dec (as per SPE)
Number of cross office priorities focussed on globally identified privacy trends or systematic issues.	3	2
Number of published “insights” reports on trends that the office is seeing.	1 In December 2021, the Office published an Insights Report on Privacy Breach Reporting.	1

Output 2 – Communication and Education

Measure	Achieved As at 31 Dec	Expectation As at 31 Dec (as per SPE)
Education module completions as a percentage of education module registrations in the year.	80%	75%
Percentage uptake on media comments made by the Office.	54% Of the 114 media enquiries received in the period to 31 December, the Office provided substantive comment on 91. Of this 91, 49 were then included in reporting.	95%
Percentage of media enquiries that are responded to within 2 working days.	97% Of the 114 media enquiries received in the period, 111 were responded to within two working days.	100%
Respond to all enquiries within 2 working days.	93%	95%

Output 3 – Compliance and Enforcement

Measure	Achieved As at 31 Dec	Expectation As at 31 Dec (as per SPE)
The percentage of data breach notifications received through NotifyUs that are triaged within 1 working day.	95%	95%
The percentage of externally reviewed compliance notices and Access Directions issued that meet quality review standards.	No reviews have taken place in the first half of the year. This will be reported on at year-end.	100%
The percentage of information matching files reviewed within the mandatory 5-year period as required under S184 of the Privacy Act.	N/A – no information matching provisions were due a 5-year review in the 6 months to 31 December.	100%

Output 4 – Advice and Advocacy

Measure	Achieved As at 31 Dec	Expectation As at 31 Dec (as per SPE)
The percentage of externally reviewed policy and information sharing are rated as 3.5 out of 5 or better for quality.	Measured at year-end.	85%
The Commissioner actively contributes on advice, guidelines and directions by international institutions and guiding bodies, relating to the advancement of privacy rights.	The Office of the Privacy Commissioner has continued to support the development of international advice, guidelines, and directions, over the past quarter. A major commitment of the office was attendance at the Global Privacy Assembly conference in October. The conference is a major event in the global privacy calendar, and the OPC contributed papers and speakers to key agenda items, and also moved or supported a number of non-binding resolutions. From 1-3 December, OPC attended the Asia-Pacific Privacy Authorities (APPA) Forum. APPA continues to be a useful regional forum for OPC to engage with, and we provided members updates on a range of local privacy matters, including our close involvement with public agencies on New Zealand's	Achieved

Measure	Achieved As at 31 Dec	Expectation As at 31 Dec (as per SPE)
	response to Covid-19 to ensure that health initiatives are designed with privacy in mind.	


Output 5 – Investigations and Dispute Resolution

Measure	Achieved As at 31 Dec	Expectation As at 31 Dec (as per SPE)
The percentage of notified complaints files closed by settlement between the parties.	63%	40%
The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality.	Measured at year end.	90%
The percentage of complaint files closed during the year that were less than 6 months old at closure.	72%	85%

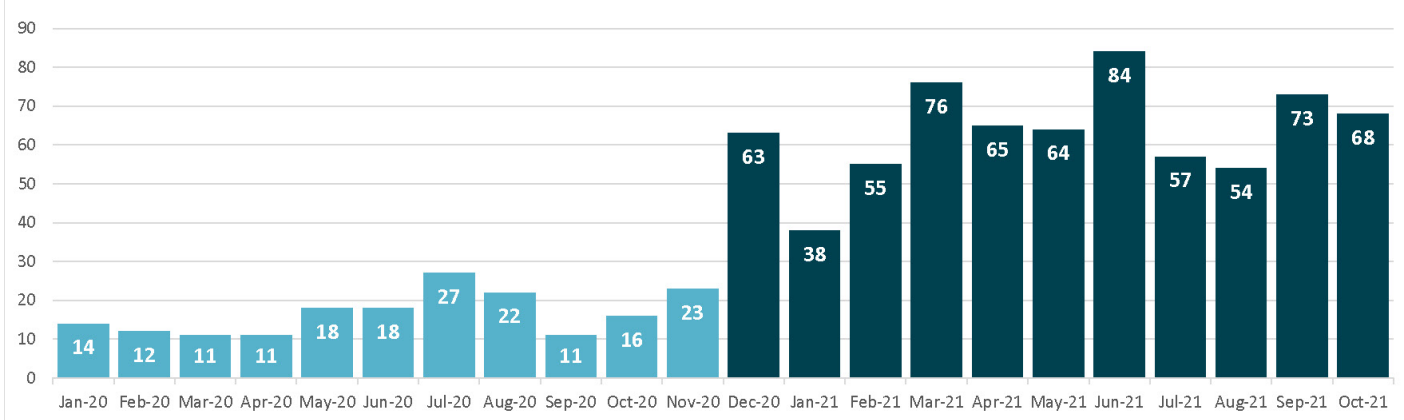
Mandatory privacy breach reporting one year on

1 December 2020 - 31 October 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 31 October 2021, we received a total of 697 privacy breach notifications, nearly four times as many as between 1 December 2019 and 31 October 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) ● Privacy Act 1993 ● Privacy Act 2020



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 31 October 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 31 October 2021, 35% 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	35 %
Reputational harm	14 %
Identity theft	13 %
Financial harm	11 %
Threats of harm	5 %
Employment harm	5 %
Loss of information	4 %
Discriminatory harm	4 %
Loss of opportunity	3 %
Physical harm	3 %

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.

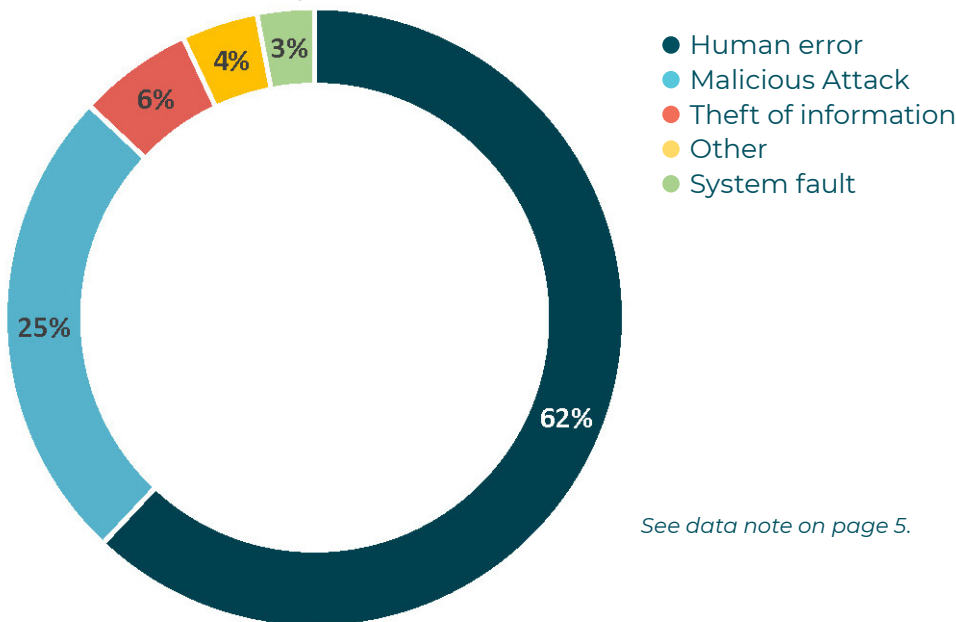
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category. Types of harm are not mutually exclusive. Hence, one privacy breach often involves more than one type of harm.

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

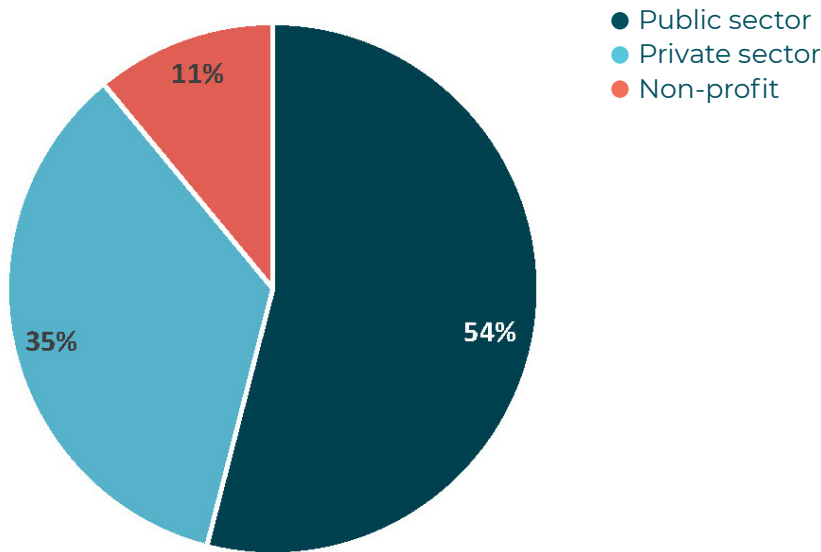
We see privacy breaches reported to us from the public, private and not for profit sectors as well as a wide range of industries. Almost all organisations hold some form of New Zealanders' personal information and they need to ensure it is well protected.

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

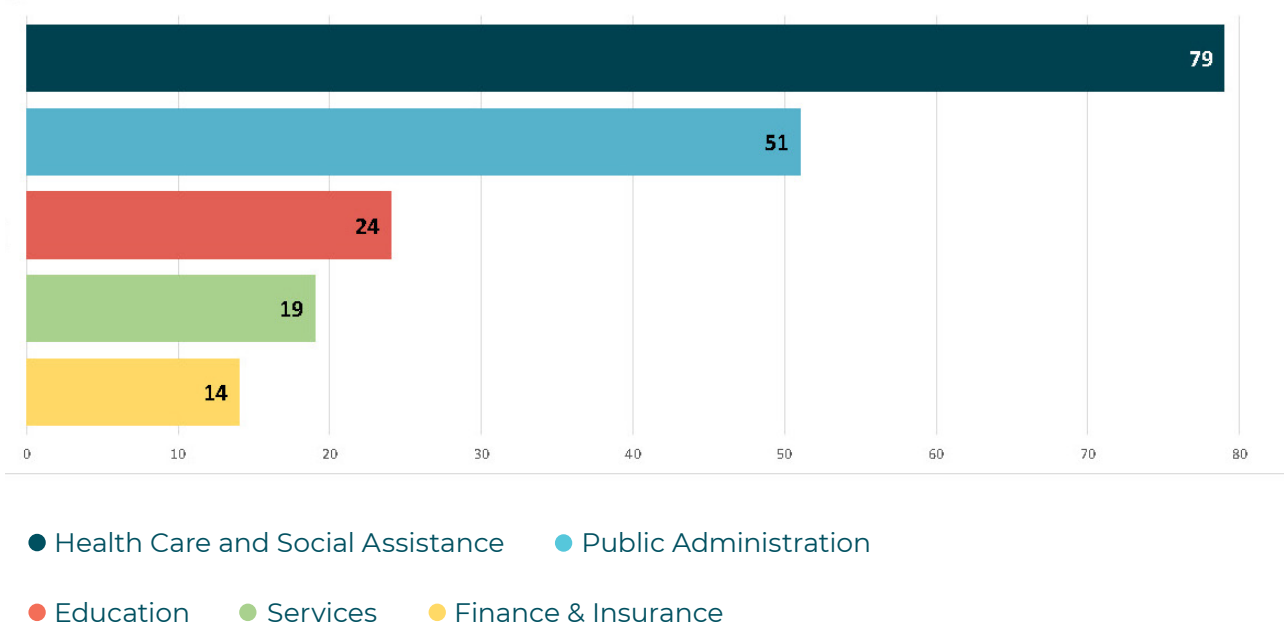
A high number of notifications from one sector or industry doesn't necessarily indicate poor privacy practice - it may mean that these sectors are more aware of their obligation to report privacy breaches.

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

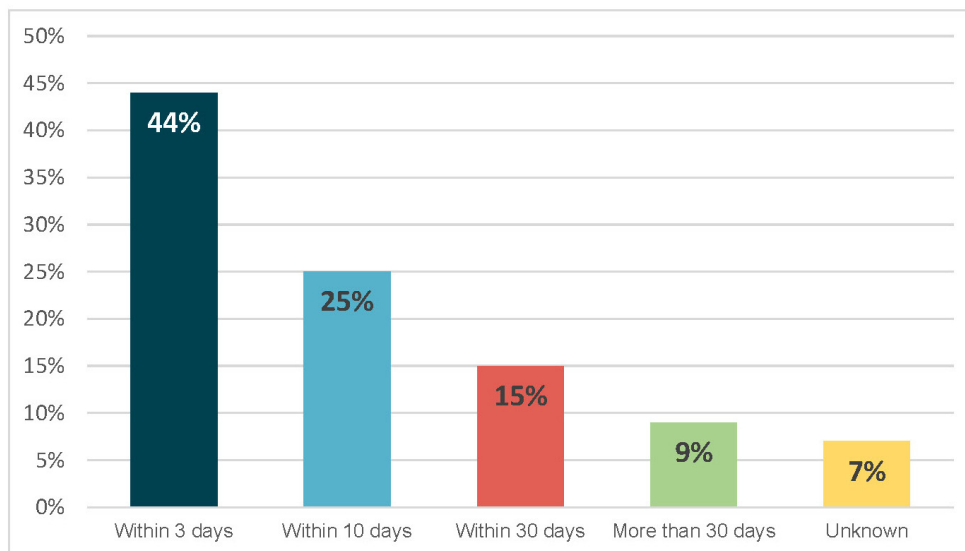


We expect you to notify us of a serious breach within 72 hours of identifying it

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



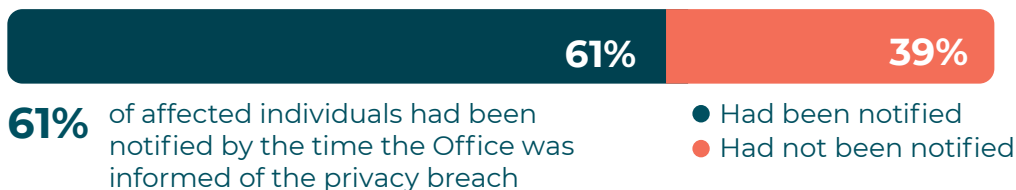
Note: 'Unknown' refers to cases when the date of identification of the breach is not known.

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 31 October 2021. NotifyUs statistics are current as of 16 November 2021. 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.

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*

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.



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



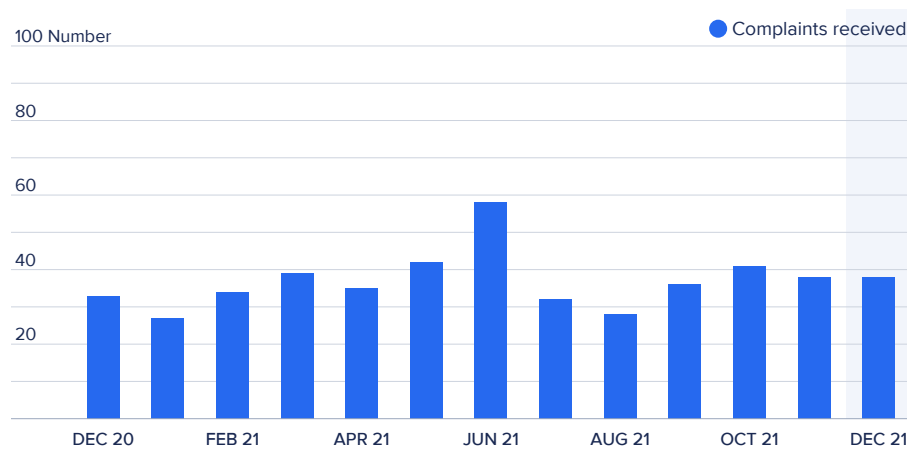


Office of the Privacy Commissioner

KPI TREND REPORT - Q2 - December 2021

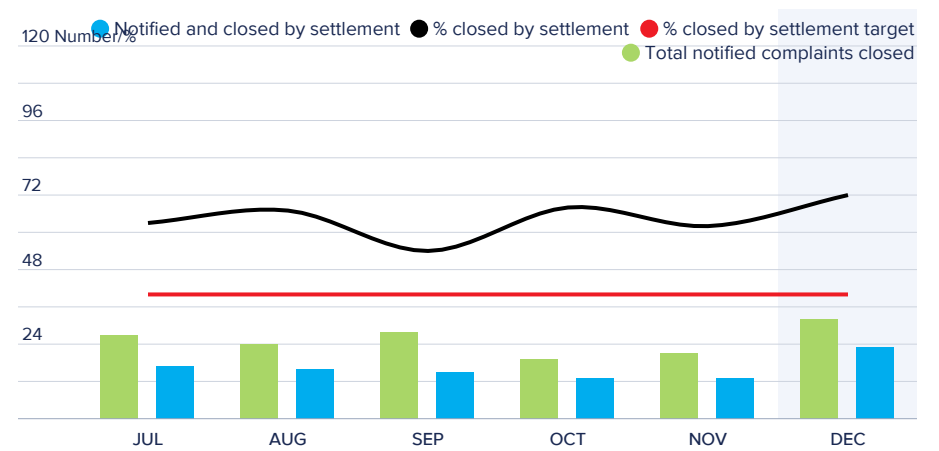
Prepared 20 January 2022

Complaints received



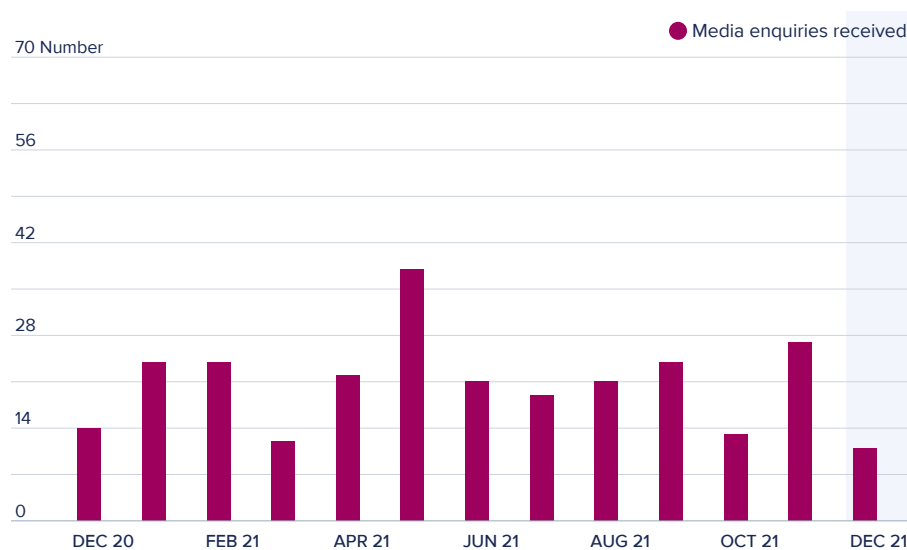
To show the trend in complaints received on a monthly basis across the year.

Closure by settlement for notified complaints (year to date)

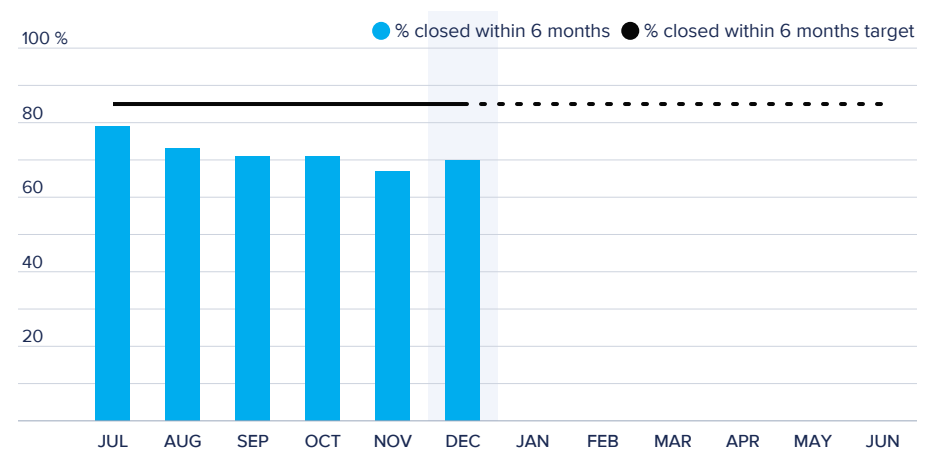


To show the number and % of notified complaints closed through settlement between the parties.

Media Enquiries received

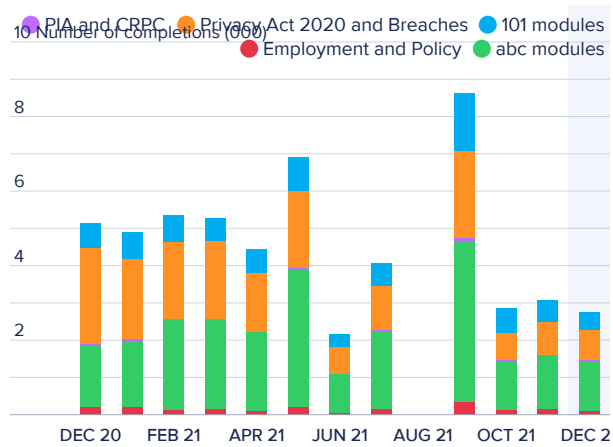


% of complaints closed less than 6 months old



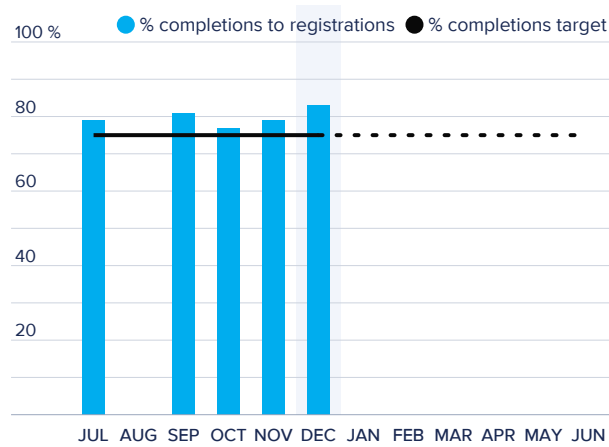
To show the % of complaints closed in the month that were less than 6 months old against the annual target of 85%.

On-line module completions



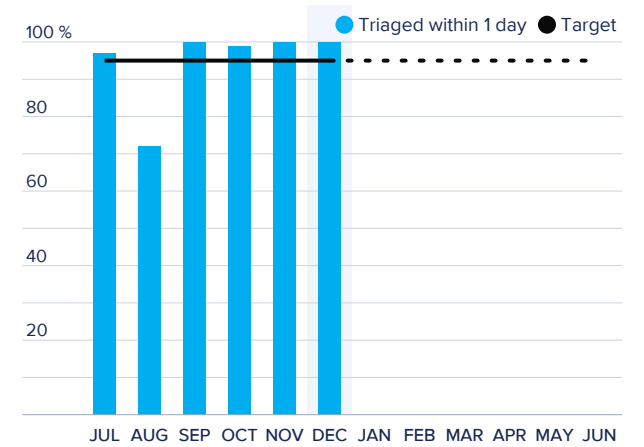
Number of monthly completions of e-learning modules.

Completions as a % of registrations



To show the monthly education module completions as a percentage of education module registrations in the month. This is shown against the annual SPE target of 75%.

Timeliness of breach triaging



To show the % of breach notifications that have been triaged with one day. This is reported against our SPE target of 95%.