Telecommunications Industry Ombudsman

Preliminary View – 5 June 2023

Deidentified

This document sets out my Preliminary View on how this complaint about the provider from the consumer should be resolved.

My Preliminary View is the provider should pay the consumer $3,500 in compensation for breaching his privacy.

The Preliminary View is what I believe to be a fair and reasonable outcome, having regard to:

- relevant laws (based on my view of what a Court would be likely to find in all the circumstances), and
- good practice, including industry guidelines.

Contents

1 Background

The consumer has a mobile service and email services with the provider.

2 The complaint and the provider's response

The consumer says that the provider allowed a third party to conduct a SIM swap of his mobile service. This third party then tried to access several different institutions where the consumer had accounts, including his bank.

His bank froze his accounts. It took approximately a month before the bank would allow him to access it again, and between it freezing the account and him gaining access again, he did not know whether the third party had stolen the significant amount of money in the account.

The consumer says the SIM swap was reversed two days later, but it had enormous impacts on his emotional and mental wellbeing and continues to impact him to this day.

The provider says it did not breach the consumer's privacy and maintains he was a victim of identity theft. It offered him $387 as a goodwill gesture.

3 The recommended outcome and the parties' response

On 6 October 2022, the TIO issued a Recommended Outcome and found:

- The provider likely breached Australian Privacy Principle (APPs) 11.1 by allowing the SIM swap to be conducted.
- Despite this, the provider had presented a fair offer to the consumer.

The consumer rejected the Recommended Outcome. He said:

- The provider had been negligent when handling his account.
- It took no action after it was notified.
- He feels its offer is unfair.

4 Reasons

In my view, the provider should pay the consumer $3,500 for its breach of the APPs. This is because:

- The provider failed to take reasonable steps to protect the consumer's personal information from unauthorised access and interference.
- The emotional and mental impact on the consumer leads to a conclusion that he should be paid $3,500.

4.1 The provider failed to take reasonable steps to protect the consumer's personal information from unauthorised access and interference.

I am satisfied the provider breached the APPs. This is because:

- The APPs require the provider to take reasonable steps to protect the consumer's personal information from access and interference.
- The provider did not take reasonable steps to prevent unauthorised access and interference.

4.1.1 The APPs require the provider to take reasonable steps to protect the consumer's personal information from access and interference.

The APPs underpin how service providers, including the provider, should handle, secure and use personal and sensitive information it holds of its customers.

APP 11.1 says:

> 'If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
>
> from interference, interference, and loss; and
>
> from unauthorised access, modification or disclosure.'

In this case, the consumer says the third party gained unauthorised access to his services and interfered with his personal information.

The Office of the Australian Information Commissioner defines 'unauthorised access' as:

> 'Unauthorised access' of personal information occurs when personal information that an APP entity holds is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity or independent contractor, as well as unauthorised access by an external third party (such as by hacking).

It also defines 'interference' as:

> ''Interference' with personal information occurs where there is an attack on personal information that an APP entity holds that interferes with the personal information but does not necessarily modify its content. 'Interference' includes an attack on a computer system that, for example, leads to exposure of personal information.'

I am satisfied allowing access to the consumer's account and permitting a SIM swap could be both 'unauthorised access' and 'interference.'

4.1.2 The provider did not take reasonable steps

In my view, the provider did not take reasonable steps to protect the consumer's personal information.

The access to the consumer's account and the SIM swap was conducted on 14 February 2022, following a call between the provider and the fraudster. The notes are recorded at 11:26am:

> Situation: wants to activate esim
>
> Action: did vision card Service number XXXX XXXXXX will receive a text to confirm the Sim replacement shortly. If the service is for data, the order will be sent directly to the bot Reference Number: [redacted]
>
> Outcome: resolved

It's also important to highlight (see the timeline of events leading up to the SIM swap in Appendix A):

- There were 4 unsuccessful attempts by the fraudster to conduct the SIM swap, before the provider allowed it. The fraudster contacted the provider an additional 3 times to reset the consumer's email password.
- On each of the unsuccessful attempts, the provider either tried to identify the fraudster and found the identity information did not match its records, or it told the fraudster to visit a store to conduct the SIM swap.
- In SIM swap cases around the time of this incident, the provider had a policy of conducting a process to verify the account holder's identity.
- On the final, and successful attempt, there are no records that the provider tried to identify the caller, nor are there records the provider's policy was followed. The provider told the TIO on 17 March 2023 that the process was not conducted, despite the notes by the representative of the provider stating one was completed.

This raises a number of issues with the way the provider approached permitting the SIM swap to occur. Over the course of two days, a third party made several attempts to access the consumer's account (8 attempts in total, with the final being successful). The provider representative on the call on 14 February 2022 at 11:26am should have:

- Identified that there were persistent unsuccessful attempts to access the account and conduct a SIM swap.
- Followed in the previous representative's footsteps, by referring the caller to the store to present their identification.

- Attempted to identify the caller (there are no notes that the representative conducted an identity check, and the provider has confirmed the call recording no longer exists).
- Followed the process according to the provider's policy at the time.
- Not recorded information on the file that was false, namely that they conducted a process when they did not.

All of these were failures to take reasonable steps to prevent unauthorised access to the consumer's account and allowed the interference of his personal information.

In addition, the provider failed to take reasonable steps in the hours following the SIM swap being conducted. Approximately 30 minutes after the SIM swap was permitted by the provider, the consumer called it. The provider noted:

> Situation: Cx contacted to enquire about the text message which he received stating that a replacement sim request was sent.
>
> Action: Checked the account and informed that there is no such message being sent from us.
>
> Outcome: Cx agreed.

This was the final opportunity for the provider to recognise the errors of the previous representative and reverse it before the SIM swap was completed. Instead, it failed to identify the problem and provided false information to the consumer. The SIM swap was completed 2 hours later.

In my view, the natural conclusion is that the provider failed to take all reasonable steps to prevent unauthorised access and interference with the consumer's personal information. It therefore breached APP 11.1.

4.2 The impact on the consumer's emotional and mental wellbeing leads to a conclusion the provider should pay $3,500 in compensation

The provider should pay the consumer $3,500 in compensation for the breach of its APPs, because:

- The TIO can award compensation for 'injury to feelings' under the *Privacy Act*.
- The consumer's emotional and mental state was impacted significantly, but there are some mitigating circumstances
- Similar decisions by the Office of the Australian Information Commissioner (OAIC) indicate $3,500 is reasonable.

4.2.1 The TIO can award compensation for injury to feelings under the Privacy Act

The framework that underpins the TIO's ability to make determinations about compensation for non-financial loss is contained in the *Privacy Act*.

Section 52 of the *Privacy Act* says the Commissioner may make a determination that a person in breach of the APPs pay compensation to someone for loss or damage. Subsection (1AB) clarifies this can relate to:

(a) injury to the feelings of the complainant or individual; and

(b) humiliation suffered by the complainant or individual.

The TIO has delegated authority from the Commissioner to also make determinations about compensation for injury to feelings and humiliation, though we do not have the power under our Terms of Reference to award aggravated damages.

When determining what is appropriate compensation for a breach of the APPs, the TIO must consider that:[1]

- Awards should be restrained, but not minimal;
- Compensation should be assessed having regard to the complainant's reaction (including injury to feelings, distress and humiliation) and not to the perceived reaction of the majority of the community or of a reasonable person in similar circumstances.

Likewise, the OAIC has outlined a number of factors in determining what is fair and reasonable:[2]

- The degree of impact on the person's mental health, including any exacerbation of mental or physical conditions.
- Whether the impacted person sought and was prescribed treatment by a doctor or psychiatrist.
- Whether the service provider took steps to mitigate any further impact, and
- The significance and degree of the breach (for example, unauthorised disclosure of sensitive information compared to a failure to protect personal information that was not of a sensitive nature).

4.2.2 The consumer's emotional and mental state was impacted significantly, though there are mitigating factors

Given the above framework, the TIO must examine the impact on the consumer and the degree of failure by the provider.

The consumer explained the impact of the breach on him, during a phone call with the

[1] See *Rummery and Federal Privacy Commissioner* [2004] AATA 1221 at [32].
[2] For example, in WP and Secretary to the Department of Home Affairs [2021] AICmr 2.

TIO on 17 February 2023. The notes of this call are as follows:

> This incident made him feel powerless, embarassed, humiliated and violated.
>
> He experienced immense anxiety and stress. It impacted himself and loved ones, especially his daughter. His daughter saw the gravity of it.
>
> The stress is all-consuming. He found the stress to be debilitating and it still makes it difficult to focus on normal tasks, as well as work.
>
> He says he's unable to enjoy activities. He's moody and irritable. He gets into arguments with his daughter - her concern is so great that it worries her and they both get into fights.
>
> He says he worries about his phone and computer security. He feels a sense of dread with notifications being received.
>
> He's also lost a sense of trust. [He needs] excessive confirmation from other people, including people he works with, that they are who they say they are.
>
> Overall, it reduced his ability to function with his everyday life and work. He needed additional support from his loved ones, including his daughter.
>
> He's had difficulty sleeping and has sporadic thoughts about this happening again.
>
> He lost trust in the provider and other organisations to implement appropriate safeguards.

I accept the consumer's statement about the impact on him and his family. It is clear that the incident has had a significant impact on his emotional and mental wellbeing.

I also consider that there are mitigating factors in this complaint:

- The provider restored the consumer's access to his mobile service within two days.
- The consumer has not sought medical treatment for his anxiety, stress and irritability.
- The breach was a result of the provider failing to take action. It was not its positive action that caused the access and SIM swap to occur, but its failure to take reasonable steps.

As a result, I consider that it is appropriate the consumer be awarded $3,500 in

compensation for the provider' failure to take reasonable steps to protect his privacy.

4.2.3 Similar decisions indicate $3,500 is reasonable

An award of $3,500 is consistent with other determinations made by the OAIC and the Administrative Appeals Tribunal. Some notable cases include:

- In *Rummery and Federal Privacy Commissioner*, the Administrative Appeals Tribunal found Mr Rummery should be entitled to compensation of $8,000. It made this finding because his employer had disclosed information about Mr Rummery's character and conduct to the ACT Ombudsman. Mr Rummery was so distressed he terminated his employment.

- In *CP v Department of Defence,* the Privacy Commissioner awarded $5,000 to a defence officer for the Department of Defence's disclosure of a psychologist's report to the complainant's treating doctor against his wishes. The defence officer's levels of anxiety, depression and stress were already 'extremely severe' prior to the disclosure. The officer also had a mood disorder that was exacerbated by the issue.

These two cases are different to the consumer's, for a few reasons:

- In *Rummery*, Mr Rummery ceased his employment and suffered significant levels of distress. The TIO consumer has suffered distress and continues to feel a sense of anxiety about the violation of his privacy by a third party, but he has not voluntarily ceased his employment.

- In *CP*, the Department of Defence disclosed highly sensitive information about the officer, which exacerbated a pre-existing mood disorder. The officer sought additional psychological treatment as a result. The TIO consumer told me he has not sought medical treatment for the distress he has experienced.

With these cases as guidance, I assess that the provider' degree of failure is lower and the consumer's degree of impact is less than both cases. It's my view an award of $3,500 is consistent with these decisions.

Senior Lead – Dispute Resolution

Telecommunications Industry Ombudsman

Appendix A

Date and time	Medium	Note
12 Feb 2022, 2:56pm	Phone	S - cx need a temporary password for his provider email xxxxxx@xxxxxxxnet.com.au A: - id not ok; details provided does not match on file - advise to visit the provider store to update his details due to Security and Data Privacy O: - not resolve
12 Feb 2022, 3:11pm	Phone	Situation Customer wanted to reset web mail password Action no access to UMT, or no one else on floor with access Outcome transferred to fixed tech
12 Feb 2022, 4:30pm	Phone	id ok. cx wants to change his number to esim. cx disconnected.
12 Feb 2022, 4:38pm	Chat	Situation Customer wanted to change to eSIM Action edu to contact us over the phone Outcome resolved
12 Feb 2022, 6:11pm	Chat	"UrgentI got a message that a password has been changed" -informed cx that the email si the same that cx uses to log in -informed would get the passwrd reset -no response -chat closed
14 Feb 2022, 10:12am	Phone	>>Situation: Cust called in because wanted to switch to esim >> Action: Checked and found that customer don't have that mobile Advised to visit nearest the provider store Cust said that he is overseas and disconnected call Called back spoke to cust and apologized and informed that for the security purpose we won't be able to activate esim cust agreed >>Outcome: Service status provided.
14 Feb 2022, 10:48am	Phone	Situation: CX is looking for e-sim QR code Action : Educated CX to visit nearest store or call our voice team. Outcome: IR
14 Feb 2022, 11:26am	Phone	S: wants to activate esim A:[checked] Service number XXXX XXX XXX will receive a text to confirm the Sim replacement shortly. If the service is for data, the order will be sent directly to the bot Reference Number: XXXXXXXXXXX Outcome resolved
14 Feb 2022, 11:52am	Phone	S: Cx contacted to enquire about the text message which he received stating that a replacement sim request was sent. A: Checked the account and informed that there is no such message being sent from us. O: Cx agreed.
14 Feb 2022, 12:02pm	Phone	S: Needs help with password reset of the provider Email A: 1. As The provider main goal is your satisfaction, we have successfully reset your password within your 3 provider email provided. Rest assured moving forward, you will be able to access your provider emails 2. And for your peace

		of mind, I will be sending you an SMS as reference confirmation O: IR
14 Feb 2022, 1:51pm	Internal	SIM swap completed
14 Feb 2022, 8:24pm	Phone	Spoke with cx, he stated that he didn't request for sim replacement i advice him to reply STOP to 1510 unfortunately he cannot send a message because the service was cut off/so upon checking there's someone who change this email address/ i already put a flash note make a manual hra, and create a case in dcm/Order was successfully submitted.