Telecommunications Industry Ombudsman

How we can help with complaints about privacy

Guidance Document

Telecommunications Industry Ombudsman

Table of Contents

Who is this document for?

This document is for anyone who wants to understand how the TIO approaches complaints about privacy. It's designed to help consumers, representatives, and members of the scheme understand our work process and our expectations.

Whether you're making a complaint or responding to one, this guide explains how we work towards fair and consistent outcomes.

1. Common types of complaints involving privacy

The following is a list of common privacy complaints we can help with. This list does not cover all complaints, and we encourage all parties to contact us to find out if we can help with the complaint or concern.

1.1 Unauthorised disclosure of personal information

- Cyber criminals hack providers' servers and steal consumers' personal information (data breach)
- Personal data used to access accounts
- Providers do not remove fraudulent charges

1.2 Unauthorised transfer of services

- Mobile services transferred to someone else without consent
- Fraudulent SIM swaps causing loss of phone numbers
- Incomplete identity authentication helped fraudster buy phones

1.3 Privacy complaints involving non-financial loss

- Disclosure of addresses
- Disclosure of personal information

Telecommunications Industry Ombudsman

2. How we handle complaints

When handling complaints about privacy, we uphold fair procedures and practices in all aspects of our work. We engage with all parties in a clear, independent and transparent way. We seek to build trust and collaboration through our engagement with all parties.

We use common approaches that help resolve complaints to do this. The following examples show how we may resolve cases. The examples are guides only. What is fair and reasonable depends on the individual circumstances of each complaint.

2.1 Unauthorised disclosure of personal information

Consumers' personal information held by providers has been accessed by unauthorised people. This is called a data breach. Unauthorised people may then use the stolen personal information to access consumers' accounts, either with their providers or banks. Consumers may also complain about fraudulent access to their accounts that did not result from a data breach but resulted in charges on their accounts.

Fraudulent activity can cause consumers to lose money and their sense of security.

Data breaches

Where data breaches happen, we expect providers to quickly investigate any unauthorised disclosure of personal information and tell consumers what personal information has been exposed. This is so consumers can take steps to protect themselves. This might be, for example, by changing passwords, freezing accounts and telling banks or other financial institutions about data breaches.

We expect providers to offer consumers alternative services, including new numbers or email addresses, to prevent further unauthorised access to accounts.

In handling complaints about data breaches, we may ask providers to show us when and what alternative services they offered consumers. We may ask providers what they did to prevent further unauthorised access to accounts. We also ask them how they responded to safeguard personal information from further breaches.

We use these responses to help us decide if providers breached any legal obligations, as well as what fair and reasonable resolutions might be in the individual circumstances of each complaint.

Fraudsters access accounts

Where unauthorised people access consumers' accounts, it's important to remember both parties may have been defrauded by third parties. We ask providers and consumers what they think happened. We ask both parties if they know who the fraudsters are and how fraudsters stole the personal information to access accounts.

We may ask providers if they noticed unusual activity on accounts. For example, if they accepted changes of details, such as switching from one preferred method of contact to another or changes of residential and email addresses. We will ask to see the providers

account notes and interaction records and ask the provider to confirm how they took reasonable steps to avoid unauthorised access, such as authentication processes and other security measures.

We may ask consumers if they shared their personal information with anyone and if they received any goods at their address. If they did, we may ask if they reported it to providers.

We would also assess the consumers individual circumstances to determine if they were more at risk to fraud than other consumers, if the provider should have been reasonably aware of this and what steps each party took to protect the information and account.

We use these responses to help us decide if providers breached any legal obligations or if they followed their own internal procedures., as well as what fair and reasonable resolutions might be in the individual circumstances of each complaint.

Solutions

Where providers have experienced data breaches, we may ask them to offer consumers compensation based on the impact unauthorised access to their personal information had on them.

If fraudsters have gained access to consumers' accounts and we find providers breached obligations, we may ask providers to overturn contracts and offer consumers compensation based on the impact unauthorised access to their personal information had on them.

If we do not find providers breached obligations or we cannot say if fraud occurred, and if we find charges are valid, we may decide consumers are responsible for the costs. In such cases we carefully consider all the circumstances before reaching a decision. We understand this may be challenging for some consumers.

If we find both parties contributed to situations where unauthorised access to accounts was made and resulted in charges, we may ask both parties to share any costs.

Case study: Simon suspected someone was interfering with his mobile account but Dialling denied it

Simon was an account holder with Dialling. He reported issues with his mobile service to Dialling. He experienced blocked calls and couldn't make outgoing calls on his mobile service. He told Dialling he suspected someone set up services in his name about a year ago without his authorisation because in Dialling's app he saw a mobile number and an email address unknown to him and had to pay additional charges. Dialling said its fraud team investigated the account and found no evidence of external control but removed the mobile number and email address and waived the charges. He asked Dialling to put a lock on his account.

Despite Simon's efforts to resolve the issue, including hiring a telecommunications technician who said someone had control of his phone, Dialling's responses failed to resolve the issues. Simon wanted to be sure his account was secure, so he complained to us.

We asked Dialling what it had done to resolve Simon's complaint. It said its fraud team investigated and found no evidence of anyone controlling the phone remotely. It said Simon must have set up the mobile number and email address by mistake and waived associated charges of $150.

We asked Dialling to give us account notes for the last two years. We found entries in the notes from around the time Simon first reported issues that had no identifying staff code but clearly showed the addition of the mobile number and service. We also found the removal of the lock Simon asked Dialling to put on his account, again with no identifying staff code.

We asked Dialling to make Simon an appropriate offer and it refused to do so.

In a Fair and Reasonable Assessment, we recommended Dialling pay Simon $2,500. This was because Dialling's records showed the mobile service was added without Simon's authorisation, Dialling did not take reasonable steps to protect Simon's personal information when it allowed the mobile service to be added by someone it could not identify, and Dialling had not adequately responded to Simon's concerns.

Both parties accepted the Fair and Reasonable Assessment.

2.2 Privacy complaints involving non-financial loss

We deal with complaints where unauthorised disclosure of personal information has happened. Where consumers have been affected by privacy breaches resulting from unauthorised disclosure, they may feel distress, anxiety, and fear for personal safety, especially in complaints involving domestic and family violence. The impacts are collectively known as non-financial loss.

Protecting personal information

We expect providers take appropriate steps to ensure the personal information of all current and previous customers' is protected from unauthorised use or disclosure.

We may ask providers to tell us what steps they take to protect personal information. We may ask providers to show us the security measures they have in place limit or prevent these situations happening. This may include monitoring accounts, training staff and proactively blocking unusual or suspicious interactions.

We expect providers to comply with legal and regulatory requirements. This includes the storage of information, sufficient procedures and measures to ensure the ongoing security of all information, and sufficient training of staff in their control.

In handling complaints about the disclosure of personal information, we may ask providers to give us account records and interaction notes. We may assess if providers met their obligations and share our findings. At a minimum, we expect provider policies and procedures seek to eliminate the risk of any unauthorised disclosure of people's personal information. We may assess the gravity of any breaches of these policies and procedures against the individual circumstances of each complaint.

Corrective and future steps

We expect providers to take all necessary steps to fix situations without hesitation or delay and to satisfy us that this has occurred. This includes acting on any immediate safety and security concerns as soon as possible. We may decide it is appropriate for providers to bear some, or all, the costs associated with remedying these immediate concerns.

For example, if the addresses of people have been disclosed and this results in any harm to the physical and psychological safety of those people, we may ask providers to bear the costs of relocation.

We may ask providers to do this immediately and while an investigation is ongoing.

We expect providers to take further steps after dealing with immediate safety and security concerns. These steps should stop any further disclosure and provide remedies for any other concerns consumers may have.

In considering what is fair and reasonable in the individual circumstances of complaints, we may consider if it is appropriate to award affected consumers compensation for non-financial loss.

Solutions

If we find providers have not met their obligations to protect personal information and personal information has been disclosed, we may ask providers to bear some or all the costs of remedying the concerns of consumers.

If we find providers have not met their obligations to protect personal information and personal information has been disclosed and caused harm to the physical and psychological safety of consumers, we may ask providers to bear some or all the costs of remedying the concerns of consumers, as well as compensating them for non-financial loss.

We assess compensation for non-financial loss against the impact disclosure of personal information has had on affected consumers.

Case study: Tellyfone transferred Aiko's services without her permission

Aiko had a mobile service with Tellyfone. In January 2024 she got a text from Tellyfone saying it had received a request to change ownership of the service. She immediately called Tellyfone and said she did not approve the change. She asked if Tellyfone if her former husband Kenji requested the change. Tellyfone said it was. She again said she did not approve the change.

Later that day Aiko's mobile and internet services were disconnected. She left work and went to the local Tellyfone store, where they told her she could not access the account as it was now in Kenji's name. Aiko went to the police station and reported what had happened.

The next day she went to the Tellyfone store again and it transferred the services back into her name. She missed three days of work and was deeply distressed by the event. She complained to us, saying Tellyfone breached her privacy.

Tellyfone tried to resolve Aiko's complaint with an offer of $500. Aiko rejected it. She said she had a restraining order against Kenji and was freshly traumatised by even hearing his name.

We asked Tellyfone for its account records and interaction notes and asked for its version of events. Tellyfone said it made a mistake with changing ownership, but it had not breached Aiko's privacy, and it restored the services one day later. Tellyfone said its Terms say it doesn't need to compensate her.

In a Fair and Reasonable Assessment, we recommended Tellyfone resolve the complaint by paying Aiko $4,500. This is because we found Tellyfone breached Aiko's privacy when it mistakenly transferred her services to her former husband. We asked Tellyfone to pay $1,500 to remedy Aiko's three days off work and $3,000 to compensate her for non-financial loss in the inconvenience, distress and trauma it caused her.

Both parties accepted the Fair & Reasonable Assessment.

3. Laws, Codes and relevant information

The laws, codes and relevant information below are what we will consider in complaints involving privacy.

- Australian Consumer Law
- Australian Privacy Principles
- Australian Privacy Principles Guidelines
- Debt Collection Guidelines for Collectors and Creditors 2021
- Privacy Act 1988
- Telecommunications Act 1997
- Telecommunications Consumer Protections Code 2019
- Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- Telecommunications Service Provider (Customer Identity Authentication) Determination 2022
- TIO Terms of Reference 2025

TIO Good Industry Practice

Our Good Industry Practice Guide for Privacy sets out what we think is good industry practice for complaints about faults with services and equipment. We expect providers to respond to consumers experiencing privacy appropriately, tailoring solutions for the individual circumstances of each complaint.

The Good Industry Practice Guide for Privacy sets out our expectations of providers under these headings:

- General handling of privacy complaints
- Unauthorised disclosure of information
- Unauthorised access to personal information
- Denying requests for personal information
- Incorrect personal information
- Unwanted communications
- Unreasonably keeping data.

Please see the TIO Good Industry Practice Guide for Privacy.