Telecommunications Industry Ombudsman

How we can help with complaints about scams, spam and fraud

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 scams, spam and fraud. 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 about scams, spam and fraud

The following is a list of common complaints about scams, spam and fraud 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 Fraud

- Unauthorised people ordering and transferring services
- Identity theft

1.2 Spam

- Calls, emails and texts from unknown people and organisations
- Phishing and malware emails or texts

1.3 Scams

- Unknown people sending texts with links to websites
- SIM card swaps

Telecommunications Industry Ombudsman

2. How we handle complaints

When handling complaints about scams, spam and fraud, 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.

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 Fraud

The most common complaints consumers make about fraud are where unknown people order and transfer services. Fraud in the telecommunications space may be any type of transaction not authorised by account holders or end users. Fraud includes cybercrime, hacking, data breaches and identity theft.

Report and recover

When consumers report fraud, we expect providers to refer them to ID Care, Report Cyber and ScamWatch so they can take immediate steps to protect their identities, report events and prevent further access to their personal information.

In handling these complaints, we may ask providers to show us they referred consumers to relevant reporting resources.

Prevent

We expect providers to help prevent fraud by using multi-factor authentication before letting anyone make significant changes to accounts, such as ordering new services.

When handling these complaints, we may ask providers to show us they did multi-factor authentication. We may ask providers to tell us how third parties accessed accounts and what steps they have in place to limit or stop such activity and what steps they took to prevent further fraudulent activity.

We ask providers to share information with consumers about fraudulent activity on their accounts so they can understand what personal information was accessed and take steps to prevent further fraudulent activity, such as changing passwords or changing phone numbers and email addresses.

Where consumers are victims of fraud, we expect providers to take preventative steps across all known accounts consumers have with them. We may ask providers to show us the preventative steps they have taken.

We use this information to help us decide what fair and reasonable resolutions might be in the individual circumstances of each complaint.

Stop credit action

Where consumers tell providers unknown people have bought products or transferred services on their accounts, we expect providers to take what they say seriously and respond

by immediately stopping all credit action and further supply of products and transferring of services.

We ask providers to suspend all disputed charges while complaints are ongoing with them or external bodies, such as the TIO or the Australian Financial Complaints Authority. We may also ask providers to separate undisputed and disputed charges.

In handling complaints about fraud, we ask providers to show us they have done this.

We use this information to help us decide what fair and reasonable resolutions might be in the individual circumstances of each complaint.

Tell consumers about their processes

Where consumers report scams and fraud, we expect providers to tell them about their scam and fraud processes and help them through the processes. We expect providers to be able to show us what steps they took with the consumer to limit harm.

We may also ask consumers what steps they took to protect themselves and limit harm.

We use this information to assess the providers' responses and decide what fair and reasonable outcomes might be.

Financial hardship

Where consumers experience financial hardship because of fraud, we expect providers to offer them help in line with their financial hardship policies and regulatory obligations.

We may ask them to show how they shared their financial hardship policies and what help they offered consumers. Help at this point might include offering to modify plans instead of cancelling them and offering consumers help with undisputed charges.

We expect providers to explain to consumers experiencing financial hardship how disputed and undisputed charges will be separated and how they should pay undisputed charges while complaints are ongoing. We may ask them to show us they did this.

When assessing these complaints, we may ask providers if they took appropriate steps to protect consumers from fraud. If we find providers did not take appropriate steps, we may ask them to consider the appropriateness of recovering associated costs.

We use this information to help us decide what fair and reasonable resolutions might be.

Solutions

If providers did not prevent fraudulent orders of products and/or the transfer of services, we may ask them to offer consumers solutions, such as new phone numbers or email addresses or release from contract without penalty, so they can move to other providers.

We expect providers take proactive steps to reduce the impacts of fraudulent activity on consumers and ensure they have access to necessary resources to protect themselves.

If we find fraudulent activities have had unusually high impacts on consumers, we may suggest awards of compensation for non-financial loss. This will depend on the individual

circumstances of each complaint and the extent to which the provider has taken appropriate steps to address the issue.

Case study: A default listing by FunnyNet meant Jasmeen couldn't get a home loan

Jasmeen applied for a home loan with her bank, which refused her application because of a default listing for $950 from FunnyNet in December 2024. Jasmeen had never been a customer of FunnyFone. When she called, FunnyNet said in January 2024 she bought an iPad and didn't pay for it. FunnyNet said it sent her bills, overdue notices, and warnings before it default listed her in December 2024. Jasmeen complained and asked to speak to the fraud team. FunnyNet said it would call her and never did.

Jasmeen complained to us. We think good industry practice is for providers to send bills to all consumers, unless they use prepaid services. This does not depend on payment methods. We shared this expectation with TellAll, which said its billing system could only send receipts to people using services they pay for by direct debit. We suggested it add bill functionality to its system.

We asked FunnyNet for interaction notes, contracts and proof of delivery. We asked Jasmeen to send us her credit report and proof of addresses she'd lived at from 1 January 2023 to now.

We compared the addresses FunnyNet delivered the iPad to with the address Jasmeen sent us proof of. They didn't match. We checked the interaction notes from January 2024 and found the calls in which 'Jasmeen' ordered the iPad. We asked FunnyNet to send us the call recordings. The recordings showed FunnyNet did not do multi-factor authentication, only accepting a driver's licence number, which matched Jasmeen's. We shared the findings of our investigation with FunnyNet and Jasmeen.

FunnyNet accepted it had not done multi-factor authentication, and the iPad sale was fraudulent.

We asked FunnyNet to buy back the $950 debt, get the default removed and offer Jasmeen compensation for her experience.

After recalling the $950 debt and removing the default listing from her credit report, FunnyNet offered Jasmeen $1,000 in compensation.

Jasmeen accepted the offer.

2.2 Spam

Consumers complain they receive unwelcome calls, texts or emails from unknown people or companies. It's called Spam, that is, unwelcome communication that usually contains advertisements, offers or promotions.

Messages that do not have advertisements, are reminders of appointments or payments, warnings about product or service faults and inform people about services they use are likely not spam.

Unwelcome messages

We expect providers to quickly help consumers stop unwelcome messages by telling them how to block calls, emails and texts on their own accounts and joining the Do Not Call Register.

We may ask providers to tell consumers using Apple operating systems how they can report and block calls and texts, and those using Android operating systems how they can forward SMS spam to the Australian Communications and Media Authority's report line, 0429 999 888, or Telstra's 7226. We may ask them to tell consumers they can forward spam emails to report@submit.spam.acma.gov.au

When handling these complaints, we may ask providers to show us they have done this.

We expect providers have processes in place to trace the origins of unwelcome messages, even if they originate from other networks. We may ask providers to share information about unwelcome messages with originating and transit providers, as well as the Australian Communications and Media Authority.

Threatening calls

Where consumers receive calls that threaten life and personal safety, are harassing, intimidating or offensive, we expect providers to trace the source of the calls, block the sources and report the sources to police.

We ask providers to show us how they did this.

Where appropriate, we may ask providers to offer consumers help in line with their Domestic and Family Violence policies and, with consumers' permission, flag and take steps to limit harm and distress.

Phishing and malware

Consumers often receive spam texts or emails that contain links to unknown websites. When people click on these links, they may become part of scams, where the senders are trying to deceive recipients into sharing personal information, such as dates of birth, or installing malicious software (malware) on consumers' computers.

We expect providers to warn consumers about phishing and malware on their websites and in their apps. When consumers report phishing and malware spam, we expect providers guide them through their processes and offer them help.

We expect providers to share information about scam calls and texts with originating and transit providers, and the Australian Communications and Media Authority. We may ask providers to show us when and how they have done this.

We use this information to help us decide what fair and reasonable resolutions might be.

Solutions

If providers are unable to reduce spam, we may ask them to offer consumers solutions such as new phone numbers or email addresses or release them from contract so they can move to other providers. We may also ask the provider to make appropriate offers to ensure the ongoing safety and wellbeing of the consumer. This may be before a complaint is finalised.

If we find spam has had an unusually high impact on consumers, we may award compensation for non-financial loss. This depends on the individual circumstances of each complaint.

Case study: Spam overwhelms Charbel's email inbox and Cedarfone's tips don't work

Charbel had an internet service and email address with Cedarfone. He received about 10 spam emails a day from overseas companies. He reported the issue to Cedarfone and Cedarfone told him how to block spam emails in its webmail service. The solution worked for a few weeks then more spam started coming to his email address. He reported it to Cedarfone and it suggested he change his email address.

Charbel didn't want to do this as he'd used the address for 15 years and didn't want to change all his passwords and update his personal information. Cedarfone said it couldn't help him anymore.

Charbel complained to us.

We asked Cedarfone what it had done to help Charbel prevent spam from reaching his email address. It told us it had explained to Charbel how to use its webmail service to block spam and then suggested he change his email address, which Charbel had refused to do.

We asked Cedarfone what other resolutions it might offer Charbel. Cedarfone said it would release him from contract.

We asked Charbel if he had left his email address anywhere on the internet or in social media. He said it is on his company website. We suggested Charbel take the email address down and create another address for the business as exposed email addresses on the internet are often targeted by spam.

Charbel found the solution reduced the flow of spam. Cedarfone credited Charbel's account $50 for the inconvenience.

3. Laws, Codes and relevant information

The laws, codes and relevant information below are what we will consider in complaints about scams, spam and fraud

- Privacy Act 1988
- The Australian Privacy Principles
- Australian Privacy Principles Guidelines
- Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020
- Telecommunications Service Provider (Customer Identity Authentication) Determination 2022
- Spam Act 2003
- Reducing Scam Calls and Scam SMS Industry Code 2020
- Scams Prevention Framework 2025.

TIO Good Industry Practice

Our Good Industry Practice Guide for Scams, Spam and Fraud sets out what we think is good industry practice for complaints about scams, spam and fraud under these headings:

- Definitions
- Unwelcome communications
- Fraud.

Please see the TIO Good Industry Practice Guide for Scams, Spam and Fraud.