



Spend Management Tools

Spend Management Tools are services or functionalities that we offer you to assist you with managing your service expenditure and service usage. These tools include:

| Control tool | Description |
|--|---|
| <p>Call barring or call restrictions</p> | <p>Call barring, also referred to as call restrictions, are facilities that can prevent unauthorised access to certain types of telephone services. You can use call barring to manage the use of your mobile, fixed line, or SIP service.</p> <p>Call barring may be applied to some or all of the following types of calls and services:</p> <ul style="list-style-type: none"> • Premium numbers • International numbers • National (long distance) • Mobile numbers • Data, SMS, and MMS services (applicable to mobile services only) |
| <p>Opt-in services (Mobile)</p> | <p>Opt-in services relate to mobile services. An opt-in service will not allow you to access a particular service or call type until you have specifically requested to do so.</p> <p>Opt-in services include:</p> <ul style="list-style-type: none"> • Opt-in to Premium content (including calls and SMS) • Opt-in to international roaming <p>Unless you have elected to Opt in to these service types you will not be able to use your mobile device to access premium content or for international roaming.</p> |
| <p>Access to unbilled amounts</p> | <p>You can access information relating to unbilled amounts on your account. Access to such information can be made by calling our Customer Experience team.</p> <p>Please note that from time to time we do experience delays in receiving usage data from our suppliers. In some instances, information relating to unbilled amounts may not take into account data used, calls made, or SMS/MMS messages sent within the last 48 hours.</p> <p>Information supplied will not take into account any included value amounts or discounts that need to be applied at the end of the month.</p> <p>Information may exclude usage incurred outside Australia, premium services, and other third-party charges.</p> |

| | |
|---------------------------------|--|
| Service Monitoring and Alerting | <p>Bendigo Telco's SmartCentre lets you monitor your service usage. You can monitor:</p> <ul style="list-style-type: none"> • NBN data usage • Mobile broadband data (accessed via your handset or via a dongle) • Mobile voice calls and SMS • International roaming on your mobile whilst travelling. <p>SmartCentre lets you setup automatic email or SMS alerting when you reach 50%, 85% or 100% of your included value on your plan¹. You can nominate different or multiple destinations for all of your service alerts.</p> <p>For more information about this contact our Customer Experience team on 1300 228 123 or go to www.bendigotelco.com.au.</p> <p>¹ Information relating to usage alerts on your plan may not take into account data used, calls made, or SMS/MMS messages sent within the last 48 hours.</p> |
|---------------------------------|--|

Security Tools

Security tools are services we offer that will aid in the prevention of unauthorised access and use of your service. These tools include:

| Security Tool | Description | Further details / activation information |
|---|--|---|
| Call Control on your fixed line service | Call Control allows you to restrict the type of calls being made from your phone. You can still make calls to restricted numbers by using a Personal Identification Number (PIN). | For further information or to activate Call Control contact our Customer Experience Team. |
| IMEI blocking of stolen mobile phones | In the event that your handset is lost or stolen you can request your IMEI to be blocked. Your IMEI is an electronic serial number or international mobile equipment identity that is unique to each mobile handset. Once a handset's IMEI is blocked the phone will no longer be able to make calls. | To report your handset as lost or stolen contact our Customer Experience Team. If you recover your handset, contact our Customer Experience Team to reactivate your IMEI. |
| 2FA | To protect our customers from fraud and identity theft, we follow rules to authenticate their identity. Multi-factor identity authentication (MFA) processes are used for all high-risk transactions. This is to make sure the person requesting the transaction is our customer, or our customer's authorised representative. | These rules are set out in the <i>Telecommunications Service Provider (Customer Identity Authentication) Determination 2022</i> . |

For more information contact our Customer Experience team on **1300 228 123**.