Anti Fraud Policy

1 Introduction

Telecommunications fraud is a large and growing "industry" around the world. Many fraudsters are:

- using telecommunications services to commit fraud e.g. scam phone callers, and
- making fraudulent use of other peoples' telecommunications services e.g. by taking control of their phone service.

Nobody can solve the problem alone, but together we can stay safer. MATE Communicate supports government efforts to educate consumers and businesses about telecommunications security and safety, and we'll do our part by:

- following relevant government requirements e.g. the Australian Communications and Media Authority (ACMA) Telecommunications Service Provider (Customer Identity Authentication) Determination 2022
- providing practical educational information on our web site e.g. our anti-scam caller page at www.letsbemates.com.au/mate/reducing-scam-calls/
- applying anti-fraud measures such as those described in this policy.

2 Some home truths about security

2.1 Keeping safer and more secure often involves a little inconvenience

It would be nice to leave our front and back doors permanently unlocked, and never need to fiddle with keys to come and go. But it wouldn't be safe or secure. Making it harder for a burglar to enter a property can involve making it a little harder for the owner to do so.

So some anti-fraud measures may involve some extra effort on our part and on yours. We think it's worth it.

2.2 Some anti-fraud measures shouldn't be publicly explained too much

Sometimes, an anti-fraud measure will be compromised if it is too transparent. For instance, a trader might introduce a new credit card identity checking requirement to apply to high value sales, e.g. sales over $1,000 for one class of product, or over $2,000 for another. It wouldn't want to detail those figures on its web site, because a fraud could easily work out that a purchase at $990 with a stolen card won't be double-checked.

So we may do some things entirely in the background, or provide limited detailed information about others.

3 Mobile phone early warnings

3.1 Background

Some customers make a lot more calls, or send a lot more texts, than others – and that's fine. Like lots of people want to send lots of SMS votes in favour of their favourite contestant in a TV talent show, or make long calls to their best friend every day.

But very high volume use can also coincide with fraud, and we want to prevent that as far as possible. Our mobile network provider Telstra Wholesale uses several fraud prevention measures, including an 'early warning system' as described here.

3.2 How it works

Telstra Wholesale has identified some service usage points and patterns that could raise concerns that a fraudster is making use of a mobile customer's service. To minimise that risk, the 'early warning system' is as follows:

(a) There are usage alert trigger points for different service components e.g. calls to Australian numbers, or international SMS.

(b) If a MATE Communicate mobile service reaches 85% of a trigger point, they'll receive an alert message.

(c) If it's just a text or talk-hungry MATE customer, they can just call us to confirm "Hey, it's me! All OK!" – after passing our identity check, of course. We'll then know that we don't need to worry there's a fraud in progress.

(d) If we don't hear back following the alert, and the service usage hits 100% of the trigger point, that service component will be paused and the customer alerted again.

(e) Like before, if the service use is all legit, a quick call (with ID check) will have the service component un-paused. But if there's no response to either alert, we'll be safe rather than sorry, and leave the pause in place for the remainder of the billing period.

(f) Remember, if you happen to receive an alert, it's simple to let us know all's well.

3.3 The service alert trigger points

We have decided to state the specific service usage trigger points in this policy, but that may change if there's evidence that fraudsters can use that information to bypass the early warning system.

(a) Australian domestic calling minutes – you are calling a standard Australian landline or mobile number from Australia
- Customer first SMS alert is at 1,224 domestic calling minutes within 3 days.
- Customer second SMS alert plus pause on domestic calling is at 1,440 minutes within 3 days.

(b) Australian SMS – you are sending an SMS to an Australian mobile number
- Customer first SMS alert is at 850 domestic SMS within 3 days.
- Customer second SMS alert plus pause on domestic SMS is at 1,000 SMS within 3 days.

(c) International calling minutes – you are calling an overseas landline or mobile number from Australia
- Customer first SMS alert is at 1,275 international calling minutes within 3 days.
- Customer second SMS alert plus pause on international calling is at 1,500 minutes within 3 days.

(d) International SMS – you are sending an SMS to an overseas number from Australia
- Customer first SMS alert is at 255 international SMS within 3 days.
- Customer second SMS alert plus pause on domestic SMS is at 300 SMS within 3 days.

3.4 Frequently asked questions

(a) What should you do if you receive an alert?

- Make sure your service isn't being used without your knowledge.
- Is the handset where it should be?
- Is it working normally?
- Do you understand why usage of the relevant service component is high?
- Is the handset with a family member or other close person? Do they know what's going on with it?
- If all is well, call us on the number stated in the alert and easily arrange for the alert to be cancelled in our system, and any pause to be un-paused.

(b) Does an alert or a service pause affect your plan entitlements?

- No!
- If you respond to a second alert, the only effect is that a service component was paused for a short time.
- And if you respond to a first alert, there isn't even a short service pause.
- But if there's no response to either alert, a service component will remain paused until the next billing period.

(c) Why is there an automatic un-pause at the end of the billing period?

- It's a balancing act. We're trying to make life hard for frauds, with minimum inconvenience to our customers.
- We expect that, if it's a fraud that has been paused, they'll probably give up on your service. So it's hopefully safe to automatically activate a paused service component after a time.
- We wouldn't want to leave a pause in place indefinitely in case a legitimate customer inadvertently overlooked both alerts.

(d) Why do we need you to call us rather than respond by text or app?

- If a fraud has your handset and can use it, they could text back to us, or respond via the app: "It's OK".
- We need you to call so we can do ID verification (e.g. your account password or secret question) before we cancel an alert or un-pause a service component.

3.5 At a glance

MATE Communicate – anti-fraud mobile alert triggers at a glance

Service component	First alert	Second alert and pause on service component
Calls within Australia	1,224 mins in 3 days	1,440 mins within 3 days
SMS to Australian no.	850 SMS in 3 days	1,000 SMS in 3 days
International calls	1,275 mins in 3 days	1,500 mins in 3 days
International SMS	255 SMS in 3 days	300 SMS in 3 days

- Alerts and potential service pauses are anti-fraud tools.
- Alerts are by SMS to relevant service number.
- Respond to first alert to avoid any service component pause.
- If response is to second alert only, service will be un-paused on ID verification.
- See our Anti-Fraud Policy for full details.

4 High risk customer transactions

4.1 What's a 'high risk transaction'?

Under ACMA rules, a high risk transaction is one that could result in:
- you losing your service,
- a change to or disclosure of a your personal information, business information or account security information,
- adding or removing an authorised representative on your account, or
- a new recurring charge or large one-off charge on your account.

4.2 Additional identity processes apply

- Under the rules, MATE Communicate will undertake additional steps to verify that the person asking for a high risk transaction on your account is you, or a person you have authorised.
- We'll walk you through those steps if they are ever required, and there are special processes that can assist in emergencies. But the normal rule is that extra identity verification is mandatory under the law.

4.3 We need your cooperation

- MATE Communicate staff cannot process a 'high risk transaction' except in accordance with detailed rules and processes.
- These extra steps can be inconvenient – for you and us – but they have been introduced across the telco industry because they have been proven to reduce fraud.
- So we do require that customers work with us, in the case of high risk transactions, to do all that's needed under the rules.