# Scammers can slip fake texts into legitimate SMS threads. Will a government crackdown stop them?

March 20 2023

Credit: AI-generated image (disclaimer)

Are you tired of receiving SMS scams pretending to be from Australia Post, the tax office, MyGov and banks? You're not alone. Each year, thousands of Australians fall victim to SMS scams. And losses have surged in recent years.

In 2022 SMS scam losses exceeded A$28 million, which is nearly triple the amount from 2021. This year they've already reached A$4 million—more than the 2020 total. These figures are probably much higher if you include unreported losses, as victims often won't speak up due to shame and social stigma.

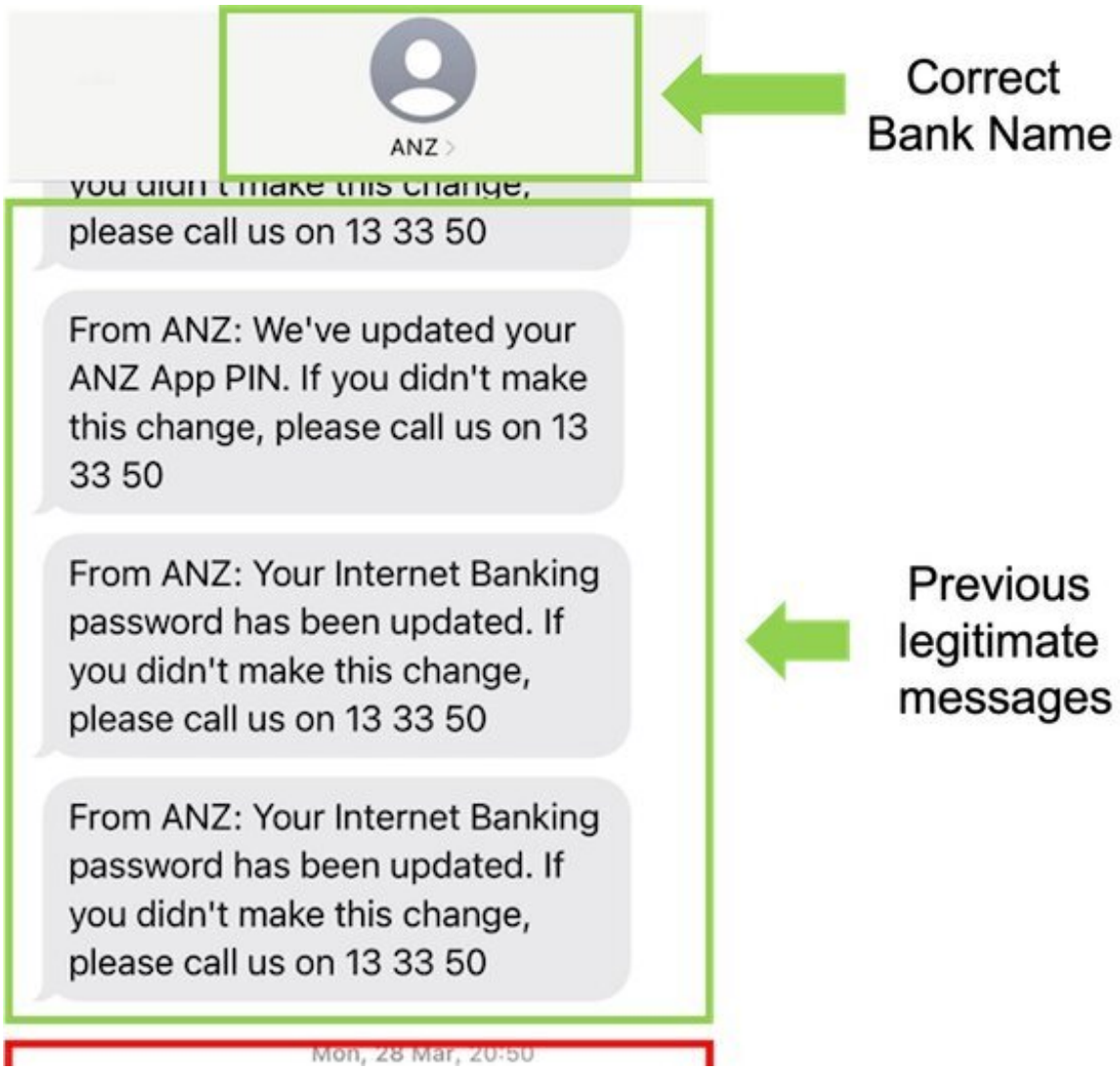
Last month, the federal government announced plans to fight SMS-based scams by implementing an SMS sender ID registry. Under this system, organizations that want to SMS customers will first have to register their sender ID with a government body.

What kinds of scams would the proposed registry help prevent? And is it too little, too late?

## Sender ID manipulation

One of the more concerning types of SMS scams is when fraudulent messages creep into legitimate message threads, making it difficult to differentiate between a legitimate service and a scam.

SMS is an older technology that lacks many modern security features, including end-to-end encryption and origin authentication (which lets you verify whether a message is sent by the claimed sender). The absence of the latter is the reason we see highly believable scams like the one below.




An example of a scam SMS message ending up in a legitimate message thread. Credit: Luu Y Nhi Nguyen

There are two main types of SMS:

- peer-to-peer (P2P) is what most people use to send messages to friends and family

- application-to-person (A2P) is a way for companies to send messages in bulk through the use of a web portal or application.

The problem with A2P messaging is that applications can be used to enter any text or number (or combination) in the sender ID field—and the recipient's phone uses this sender ID to group messages into threads.

In the example above, the scammer would have simply needed to write "ANZ" in the sender ID field for their fraudulent message to show up in the real message thread with ANZ. And, of course, they could still impersonate ANZ even if no previous legitimate thread existed, in which case it would show up in a new thread.

Web portals and apps offering A2P services generally don't do their due diligence and check whether a sender is the actual owner of the sender ID they're using. There are also no requirements for telecom companies to verify this.

Moreover, telecom providers generally can't block scam SMS messages due to how difficult it is to distinguish them from genuine messages.

## How would sender ID registration help?

Last year the Australian Communications and Media Authority introduced new rules for the telecom industry to combat SMS scams by tracing and blocking them. The Reducing Scam Calls and Scam Short Messages Industry Code required providers to share threat intelligence about scams and report them to authorities.

In January, A2P texting solutions company Modica received a warning for failing to comply with the rules. ACMA found Modica didn't have proper procedures to verify the legitimacy of text-based SMS sender

IDs, which allowed scammers to reach many mobile users in Australia.

Although ACMA's code is useful, it's challenging to identify all A2P providers who aren't following it. More action was needed.

In February, the government instructed ACMA to explore establishing an SMS sender ID registry. This would essentially be a whitelist of all alphanumeric sender IDs that can be legitimately used in Australia (such as "ANZ", "T20WorldCup" or "Uber").

Any company wanting to use a sender ID would have to provide identification and register it. This way, telecom providers could refer to the registry and block suspicious messages at the network level—allowing an extra defence in case A2P providers don't do their due diligence (or become compromised).

It's not yet decided what identification details an Australia registry would collect, but these could include sender numbers associated with an organization, and/or a list of A2P providers they use.

So, if there are messages being sent by "ANZ" from a number that ANZ hasn't registered, or through an A2P provider ANZ hasn't nominated, the telecom provider could then flag these as scams.

An SMS sender ID registry would be a positive step, but arguably long overdue and sluggishly taken. The UK and Singapore have had similar systems in place since 2018 and last year, respectively. But there's no clear timeline for Australia. Decision makers must act quickly, bearing in mind that adoption by telecom providers will take time.

## Remaining alert

An SMS sender ID registry will reduce company impersonation, but it

won't prevent all SMS scams. Scammers can still use regular sender numbers for scams such as the "Hi Mum" scam.

Also, as SMS security comes under increased scrutiny, bad actors may shift to messaging apps such as WhatsApp or Viber, in which case regulatory control will be challenging.

These apps are often end-to-end encrypted, which makes it very difficult for regulators and service providers to detect and block scams sent through them. So even once a registry is established, whenever that may be, users will need to remain alert.



Provided by The Conversation