

Media release

15 August 2023

Burst SMS breached for allowing scams

Sydney-based business Known Pty Ltd (trading as Burst SMS) has breached SMS anti-scam rules by allowing scammers to send messages impersonating well-known Australian brands, including financial institutions, telcos, couriers, ride share and ticketing companies.

An Australian Communications and Media Authority (ACMA) [investigation](#) found Burst SMS offered its customers a free trial to send up to 10 messages a day without undertaking required checks, during which time scammers sent 108 SMS across a 1-month period using text-based sender IDs (i.e. a business name) impersonating reputable businesses.

Text-based sender IDs can be used by scammers to pose as legitimate organisations such as government agencies, banks and road toll companies. Under the Reducing Scam Calls and Scam SMS Code, Australian telcos must obtain evidence from customers that they have a legitimate reason to use text-based sender IDs in SMS.

ACMA Chair Nerida O'Loughlin said scams that use fake text-based Sender IDs can be particularly hard to spot.

"Scammers will take advantage of any small crack in the system, and on this occasion they took the opportunity opened up by Burst's free trial offer," she said.

"Every text that contains a link should be treated with caution until you are sure it is legitimate. If there is any doubt then the best course of action is to report and delete the message."

The ACMA has directed Burst SMS to comply with the code and if future breaches are found, the telco may face stronger enforcement action such as commencement of proceedings in the Federal Court.

The code requires telcos to identify, trace and block suspected SMS scams, and to conduct checks on organisations using text-based sender IDs. Since the rules were introduced in July 2022, Australian telcos have reported blocking over 257 million SMS scams to the end of June 2023.

Combating SMS scams is an ACMA compliance priority, and telcos may face penalties of up to \$250,000 for breaching ACMA directions to comply with the code. This action follows an [announcement in May](#) about other telcos providing bulk SMS services that had breached the same obligations.

The ACMA is currently working with the telco industry to develop an SMS sender ID registry to provide further protections against scammers impersonating trusted brands and government agencies.

The SMS Sender ID Registry is part of the Government's Fighting Scams initiative to address scams and online fraud, to protect Australians from financial harm. The initiative also includes the establishment of the National Anti-Scam Centre, which commenced operations on 1 July 2023.

If you think you've been scammed, contact your bank and phone company immediately [and report it to Scamwatch](#). Contact [IDCARE](#) if you've had personal details stolen.

For information on how to spot – and stop – phone scams, visit acma.gov.au/scams.

MR 24/2023

For more information, please contact ACMA Media on 0438 375 776 or media@acma.gov.au.



acma.gov.au

**Australian
Communications
and Media Authority**

[View online](#) | [Unsubscribe](#) | [Manage your subscriptions](#) | [Our newsletters](#) | [Contact us](#)