Members of the media are welcome to re-phrase the information contained in this media release, but the essential information at time of distribution is correct and should not be altered.

DATE Tuesday 23 February 2010 TIME 1030

"Phreaking" Investigation

Detectives from the South Australia Police, Electronic Crime Section, have been investigating a recent incident involving a local Adelaide business and hundreds of unauthorised phone calls billed to their account. "Phreaking", otherwise known as 'dial-through fraud' or 'toll fraud', is the fraudulent and illegal use of a company's telecommunications system by a third party from a remote location. A Voice over Internet Protocol (VoIP) telephone system or a Private Automatic Branch Exchange (PABX) is common place among many businesses to manage their telephone needs. Some systems arrive setup with default features that can be exploited by criminals, such as call forwarding. Once a phone system has been compromised by criminals, calling cards are sold and distributed in overseas countries, often to unsuspecting members of the public, which are in turn are used to call any number of foreign countries. A compromised phone system will call through several other compromised systems until connecting to an unsuspecting member of the public overseas. Telephone bills can add up extremely quickly and the more outgoing lines available the more people can connect and dial out. In several interstate cases phone bills in excess of $100,000 are being charged. Telephone carriers are not liable for these call charges as it is the responsibility of each company's IT consultant to secure their system as they would secure their internet connection and local area network from outside intruders. Tracking down offenders is difficult as the criminal behaviour originates from overseas. SAPol recommends all business owners review their policies regarding this often forgotten side of their infrastructure and ensure their system is secure. This can include disabling features of the phone system that are not used by their business, changing the default passwords to something much stronger and restricting 1900 and overseas calls from being dialled if this service is not used.

AUTHORISED BY Detective Superintendent Jim Jeffery – Commercial and Electronic Crime Branch
MEDIA OFFICER Senior Constable Dave Muir
MEDIA SECTION TELEPHONE 8226 26 88 FACSIMILE 8463 3723