

Introduction

What is a Chinese Authority Scam?

This scam targets Chinese Australian communities and international students by impersonating Chinese police or other government officials. The scam commences with a phone call suggesting involvement in illegal activity and comes with threats of arrest or deportation, along with financial extortion and demands for identity documents.

Prevention

How can I avoid being involved in a Chinese authority scam?

- ☐ Be vigilant when receiving unsolicited calls.
- ☐ Be suspicious of any sense of urgency being placed upon you to act.
- ☐ While the number may appear to be legitimate – hang up and contact the organisation on their verified number.

Detection checklist

If you are concerned that you or someone you know may be involved in a Chinese authority phone scam this checklist can help you identify the red flags:

The more boxes you tick, the more likely it's a scam.

- ☐ You received a robo-call with a pre-recorded message impersonating police, prompting you to press 1 to speak to an operator. However, some individuals reporting to IDCARE state the scam started with a real time unsolicited phone call.
- ☐ The caller claims you have been involved in illegal activity and must comply with their requests.
- ☐ The caller has alleged that you have set up a phone account to scam others or have committed identity fraud.
- ☐ The caller uses threats of arrest or deportation if you don't comply.
- ☐ The caller demands that all communication must happen in private and that you must not discuss the case with anyone else, including your family members.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Detection checklist cont.

- ☐ The caller might request you move communications to an encrypted or private messaging platform.
- ☐ There may be a request for a video call where the caller is wearing a police uniform and uses their 'authority' to question you about details of your family living abroad.
- ☐ You are required to "check in" and provide updates as to your whereabouts at regular intervals throughout the day.
- ☐ There are demands for payment where you may be coerced to use your savings to transfer money or to buy cryptocurrency.
- ☐ You are directed to comply with all requests or told you risk criminal charges.

Response checklist

With this scam there is often request that you provide a photo of yourself holding your passport, national ID card, or other identity credentials. If this has happened to you:

- ☐ Cease all communication with the scammer.
- ☐ Tell a trusted person what has happened if you need support as you work through the emotional, practical, and potentially financial, recovery.
- ☐ Advise your bank(s) of the scam (if this information was provided).
- ☐ If you have had your Australian Passport exposed, you can cancel your passport and pay for a new passport with a new passport number. If you have had a Chinese passport, licence or national ID card compromised you may discover whether anyone has misused your ID in China in relation to credit applications by obtaining a copy of your credit report with the [Credit Reference Center at the People's Bank of China](#).
- ☐ If you have provided government issued identity documents, contact both credit reporting agencies for your [credit reports](#) and to request a [credit ban](#).

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Response checklist cont.

- ☐ If you have sent or received money or goods online, provided remote access to your computer, or shared credentials online that would enable identity theft and fraud, you can alert police through:
 - [ReportCyber](#) (in Australia)
 - Call 105 or [online](#) and choose "Report a Police non-emergency" (in New Zealand)
- ☐ Contact your GP if you feel you need additional support and strategies to deal with the stress of your situation.
- ☐ Be aware that you may see an increase in scam attempts.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.